Protección de datos y comercio electrónico

PID_00248514

Antonia Paniza Fullana

Tiempo mínimo de dedicación recomendado: 8 horas

Universitat Oberta de Catalunya

Índice

Introducción

Con esta introducción se pretende presentar con carácter general la materia de este módulo, que es especialmente interesante ya que conjuga la protección de datos y toda su normativa con la de contratación, comercio electrónico, protección de los consumidores y publicidad. Normativas que hay que encajar y, en ocasiones, evitar duplicidades, como podría llegar a ser el caso de las sanciones ante determinadas infracciones tipificadas en ambas reglamentaciones.

Por otra parte, el nuevo Reglamento General de Protección de Datos (RGPD) nos da algunas nuevas pautas, que ya han de tenerse en cuenta, como es la protección de datos desde el diseño y por defecto. Tampoco puede olvidarse la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto a la vida privada y a la protección de datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). El uso de nuevos conceptos como las llamadas de mercadotecnia directa, el tratamiento conjunto de los distintos medios tecnológicos para el envío de comunicaciones comerciales, el intento de introducir los avances tecnológicos, etc., son puntos a tener en cuenta en el análisis de esta nueva Propuesta.

Como se irá viendo a lo largo de este material, el **consentimiento** del interesado es un punto clave en el tratamiento de datos en general, y en la recopilación de datos para fines comerciales y envío de comunicaciones comerciales o uso de datos para fines publicitarios, en particular. Por ello, es importante, aunque ya ha sido objeto de estudio en otro módulo, recordar el concepto de consentimiento en la normativa de protección de datos. El RGPD lo define como «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». Fíjense como esta definición exige un consentimiento expreso: mediante declaración o, en general, una acción afirmativa por parte del usuario. Por su parte, el artículo 3 de la LOPDP se refiere al consentimiento como: «toda manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen». Y según el artículo 7 del Anteproyecto de Ley Orgánica de Protección de Datos, se entiende por consentimiento del afectado «toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». Salvo las excepciones, que se estudiarán en los apartados correspondientes, la regla general será la necesidad del consentimiento para el uso de datos de carácter personal de los usuarios para fines comerciales.

Y este consentimiento no puede presentarse aislado de la definición de **dato de carácter personal**. En la LOPDP se define este concepto como «cualquier información concerniente a personas físicas identificadas e identificables», mientras que en el RGPD la definición es «toda información sobre una persona física identificada e identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». Se verá que, en la mayoría de casos, los datos que se utilizan para fines publicitarios son datos de carácter personal.

Resumen de la normativa aplicable

Las principales normas que se estudiarán en este módulo son:

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 15/1999, de 13 de diciembre, que regula la Protección de Datos de Carácter Personal. Cabe señalar que existe un Anteproyecto de reforma de esta Ley.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.
- Real Decreto Legislativo 1/2007, de 16 de noviembre, que aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley 34/1988, de 11 de noviembre, General de Publicidad.
- Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios.

Además de otros textos, como la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas, disponible en: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications). Y también hay que hacer una mención al Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

A partir de la normativa aplicable, se planteará una nueva cuestión a raíz de la publicación, entrada en vigor y aplicación del Reglamento General de Protección de Datos, en lo relativo al sistema de fuentes. Esta es una norma directamente aplicable, pero hay cuestiones que no están desarrolladas, por lo que se puede plantear la aplicación de la normativa estatal sobre la materia,

por ejemplo en el caso de los ficheros de publicidad y prospección comercial, cuestión desarrollada en 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 Protección de Datos de Carácter Personal.

Sobre esta cuestión, es muy claro Piñar Mañas al afirmar que:

> «Al tiempo que se conserva la normativa estatal, horizontal y sectorial, dictada en desarrollo de la derogada Directiva 95/46/CE (con las salvedades que seguidamente se mencionan) se añade una fuente supraestatal directamente aplicable. No bastará ya pues con "tirar" de la LOPDP y el R.D. 1720/2007 para resolver nuestros problemas: habrá que hacerlo también del Reglamento, sin a la par prescindir de la normativa nacional.»
>
> J. L. Piñar Mañas (2016). «Introducción. Hacia un nuevo modelo europeo de protección de datos». En: Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (págs. 15-22).

1. Marco legal del prestador de servicios de la sociedad de la información (LSSI)

1.1. Concepto

El Anexo de la LSSICE define al **prestador de servicios** como la persona física o jurídica que proporciona un servicio de la sociedad de la información. Y un **servicio** de la sociedad de la información es «todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario». También se consideran servicios de la sociedad de la información los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios. A continuación, el Anexo pasa a enumerar una serie de servicios de la sociedad de la información. Se calificarán como tales siempre que representen una actividad económica los siguientes:

- la contratación de bienes o servicios por vía electrónica,
- la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales,
- la gestión de compras en la red por grupos de personas,
- el envío de comunicaciones comerciales,
- el suministro de información por vía telemática.

Y en sentido negativo, no tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características establecidas y, en particular:

- Los servicios prestados por medio de telefonía vocal, fax o télex.
- El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.
- Los servicios de radiodifusión televisiva.
- Los servicios de radiodifusión sonora.
- El teletexto televisivo y otros servicios equivalentes, como las guías electrónicas de programas, ofrecidos a través de plataformas televisivas.

Servicio de la sociedad de la información

Siguiendo a Camacho Clavijo, el **servicio de la sociedad de la información** puede definirse como «todas las actividades que se realicen por vía electrónica y que tengan un significado económico y lo tienen todas las actividades que se lleven a cabo por vía electrónica y que constituyan, para su prestador, el objeto de una actividad económica, sin importar que se trate de servicios no remunerados por sus destinatarios». La falta de remuneración no excluye que se trate de un servicio de la sociedad de la información, si se obtienen ingresos de forma indirecta. Véase:

S. Camacho Clavijo (2016). «Régimen jurídico de los prestadores de servicios de la sociedad de la información». En: Navas Navarro, S.; Camacho Clavijo, S. *Mercado Digital. Principios y reglas jurídicas*. Valencia: Tirant Lo Blanch (pág. 109).

Por su parte, el RGPD, en su artículo 4 destinado a las definiciones, se refiere al servicio de la sociedad de la información remitiendo al artículo 1.1, b) de la Directiva (UE) 2015\1535 del Parlamento y del Consejo.

Según este artículo de la Directiva 2015\1535, **servicio** es:

> «[...] todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.
>
> A efectos de la presente definición, se entenderá por:
>
> i) "a distancia", un servicio prestado sin que las partes estén presentes simultáneamente,
>
> ii) "por vía electrónica", un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético,
>
> iii) "a petición individual de un destinatario de servicios", un servicio prestado mediante transmisión de datos a petición individual.
>
> En el anexo I figura una lista indicativa de los servicios no cubiertos por esta definición.»

El destinatario de servicios es la persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información. En este punto, habrá que tener en cuenta la definición de **destinatario** en la normativa de protección de datos de carácter personal y la propia noción de **consumidor**, sobre todo por lo que hace referencia a la persona jurídica, cuestiones que serán tratadas más adelante.

En las relaciones que tienen los prestadores de servicios con el destinatario de los servicios de la sociedad de la información, necesitarán tratar datos de carácter personal. El prestador de servicios estará sometido a las reglas y los principios de las normas de la protección de datos cuando se usen datos de carácter personal que correspondan a personas físicas identificables, ya que la LOPDP define los **datos de carácter personal** como «cualquier información

perteneciente a personas físicas identificadas o identificables». Y El RGPD define **datos personales** como «toda información sobre una persona física identificada o identificable (el interesado)» y añade:

> «Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.»

1.2. Clases de prestadores de servicios de la sociedad de la información

Siguiendo a Payeras Capellá, los intermediarios pueden ser clasificados en función del servicio o conjunto de servicios que prestan, así como del punto en el que actúan. Por una parte, los servicios de infraestructuras prestan servicios de conexión y transmisión de datos por redes de telecomunicaciones. Por otra parte, la publicación de contenidos requiere un servicio de alojamiento en servidores de datos, servicio que puede ser ofrecido por un intermediario. Tenemos intermediarios de acceso e intermediarios de alojamiento.

Lectura recomendada

Sobre esta cuestión, véase:
M. Payeras Capellá; S. Cavanillas Múgica (2005). «Los servidores de acceso y alojamiento: descripción técnica y legal». En: Cavanillas Múgica, S. (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares (págs. 1-48).

En el Anexo de la LSSICE ya se define **servicio de intermediación** como el servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. Y enumera los servicios de intermediación: la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones, etc.

1.3. Una aproximación al régimen de responsabilidad de los prestadores de servicios de la sociedad de la información en la LSSICE

A nivel europeo se abordó la cuestión para todo tipo de contenidos en la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio de 2000, sobre Comercio Electrónico. En torno a esta cuestión se plantean cuestiones como: ¿tienen que ser responsables los intermediarios por los contenidos introducidos por terceros en sus servidores? ¿Quién debe responder de las opiniones vertidas en un foro? ¿Hasta dónde llega la libertad de expresión de los participantes en un foro o en un determinado sitio web?

En primer lugar, al abordar el tema de la responsabilidad de los prestadores de servicios, hay que tener en cuenta el artículo 13 LSSICE, que establece que los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida en el ordenamiento jurídico, sin perjuicio de lo establecido en la Ley.

Seguidamente, la LSSICE se refiere a la responsabilidad de los servicios de intermediación. Los artículos 14 y siguientes se refieren a un sistema específico de responsabilidad aplicable a estos prestadores de servicios:

1) Responsabilidad de los operadores de redes y proveedores de acceso: cuando presten un servicio de intermediación que consista en transmitir, por una red de telecomunicaciones, datos facilitados por el destinatario del servicio o en facilitar acceso a esta no serán responsables por la información transmitida, salvo que ellos mismos hayan originado la transmisión, modificado los datos o seleccionado estos o a los destinatarios de dichos datos. No se entenderá por modificación la manipulación estrictamente técnica de los archivos que alberguen los datos que tienen lugar durante la transmisión.

Según el artículo 14 LSSICE, las actividades de transmisión y provisión de acceso incluyen el almacenamiento automático, provisional y transitorio de los datos, siempre que sirva exclusivamente para permitir su transmisión por la red de telecomunicaciones y su duración no supere el tiempo razonablemente necesario para ello.

2) Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios. En este caso, se trata de prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal. En este supuesto, estos prestadores de servicios no serán responsables por el contenido de estos datos ni por la reproducción temporal de los mismos siempre que cumplan una serie de condiciones:

- No modificar la información.

- Permitir el acceso a ella solo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

- Respetar las normas generalmente aceptadas y aplicadas por el sector para la actualización de información.

- No interferir en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información.

- Retirar la información que hayan almacenado o hacer imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:
  - que ha sido retirada del lugar de la red en que se encontraba inicialmente;

– que se ha imposibilitado el acceso a ella, o

– que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella.

3) Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos. En este caso, los prestadores de servicios de intermediación, consistente en albergar datos proporcionados por el destinatario de este servicio, no serán responsables por la información almacenada a petición del destinatario siempre que se cumplan dos requisitos:

- No tener conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización.

- Si lo tienen, actuar con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Seguidamente, el artículo 16 LSSICE establece qué se entiende por **conocimiento efectivo**: se entenderá que hay conocimiento efectivo cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

Esta exención de responsabilidad no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, la autoridad o el control de su prestador.

Por lo que se refiere a la responsabilidad de los prestadores de servicios de alojamiento, se pueden encontrar muchas resoluciones sobre la cuestión. Cuestión problemática la relativa a la responsabilidad de estos prestadores de servicios por los contenidos albergados en sus páginas.

A modo de ejemplo: la Sentencia del Tribunal Supremo (STS) de 18 de mayo de 2010 («quejas online») o la STS de 9 de diciembre de 2009, en las que se aplica el artículo 16 LSSICE. Los hechos de la primera de las sentencias citadas son los siguientes: Don J.M.M. interpone demanda de juicio ordinario por intromisión ilegítima en su derecho al honor contra la empresa R. S.L. Don J.M.M. es abogado y tiene entre sus clientes a la empresa «Mutua Madrileña Automovilista», siendo esta empresa su cliente más importante desde 1991. La empresa R. S.L. es la titular del sitio web: «quejasonline», que recogía quejas contra «Mutua Madrileña Automovilista». El día 4 de junio de 2004 aparece en el mencionado sitio web el siguiente comentario suplantando a Don J.M.M. como abogado de la mencionada entidad: «Soy abogado de la Mutua Madri-

Lecturas recomendadas

Sobre esta cuestión, véase:

A. Paniza Fullana (2010). «Alcance de la responsabilidad de los prestadores de servicios de la sociedad de la información. (A propósito de la Sentencia del Tribunal Supremo de 18 de mayo de 2010)». *Aranzadi Civil. Revista Doctrinal* (núm. 4, págs. 27-36).

S. Cavanillas Múgica (2011). «Comentario a la Sentencia del Tribunal Supremo de 18 de mayo de 2010: responsabilidad de un prestador de un servicio intermediario de la sociedad de la información, de alojamiento, por la intromisión ilegítima causada por un comentario enviado a un foro». *Revista Cuadernos Civitas de Jurisprudencia Civil* (núm., 85, págs. 447-456).

leña y estoy cansado de engañar a la gente, pues la Mutua me hace retrasar los expedientes con el fin de no pagar, tiene pinta de irse al garete». Don J.M.M. comunica la situación a la empresa R. S.L. y le requiere para que retire la nota y le comunique la identidad del remitente. La mencionada empresa retira la nota pero le contesta negándose a facilitar la identidad del remitente de la misma ya que, de acuerdo con las normas sobre protección de datos, necesitaría el consentimiento del autor. Una de las cuestiones que se presentan es la dificultad del prestador de servicios de alojamiento de controlar todos los contenidos introducidos, además de plantearse si ello supondría una limitación a la libertad de expresión. Por ello, lo que hacen las normas aplicables es establecer exenciones de responsabilidad cuando se cumplan una serie de requisitos. En el caso de la STS de 18 de mayo de 2010, frente a la actitud negligente de la empresa R., S.L. que aprecian las dos instancias, el Tribunal Supremo, en aplicación del artículo 16 LSSICE, entiende que ha cumplido todos los requisitos que impone este precepto.

Especialmente interesante en estos casos es la interpretación del concepto de **conocimiento efectivo**.

Se refiere a esta cuestión y a las diferentes interpretaciones de conocimiento efectivo y a su alcance, el Fundamento de Derecho octavo de la STS de 7 de enero de 2013. En este caso, la representación de una empresa de informática «Aiguamolls Electro-Informática» interpone demanda contra «Meristation Magazine, S.L.» en defensa del honor de su representado por las expresiones contenidas en los foros de la página web www.meristation.com, tales como: «Aiguamolls también me quiere estafar, esos hijos de puta no pueden quedar impunes, leer los e-mails que te manda este sinvergüenza, menudo sinvergüenza y desgraciado, a este timador [...]».

Lo hace en estos términos:

«La cuestión litigiosa se centra en determinar si el Tribunal de apelación ha aplicado correctamente el régimen de exclusión establecido en la Directiva 2000/31/CE (LCEur 2000, 1838) y en los artículos 13.1 y 16 de la Ley 34/2002 (RCL 2002, 1744 y 1987) que incorpora al ordenamiento jurídico español tal Directiva. Tras analizar lo que dicen dichos artículos, expone las dos interpretaciones doctrinales del concepto "conocimiento efectivo" contenido en el artículo 16 de la citada Ley. Una primera, cuyos argumentos principales se encuentran en los antecedentes legislativos y prelegislativos de la ley y en su propia literalidad, y viene a sostener que, no habiéndose establecido legal ni reglamentariamente otros medios de conocimiento y a falta de acuerdos voluntarios sobre procedimientos de detección y retirada, solo podrá afirmarse la concurrencia de "conocimiento efectivo" en presencia de una previa resolución de un órgano competente acerca de la ilicitud de los datos en cuestión. La segunda considera que la Directiva de la que procede la Ley –que emplea el metro del "conocimiento efectivo" para la exención de responsabilidad penal y el de "conocimiento de hechos o circunstancias por los que la actividad o la información revele su carácter ilícito" para la que atañe a la responsabilidad civil–, el párrafo mencionado tiene naturaleza meramente ejemplificativa y no excluye que pueda probarse la existencia de "conocimiento efectivo" de cualquier otra manera.

Se muestra partidario de la interpretación más amplia acogida por esta Sala en las sentencias de 10 de febrero de 2011 (RJ 2011, 313), 18 de mayo de 2010 (RJ 2010, 2319) y 9 de diciembre de 2009 (RJ 2010, 131), entendiendo que la prueba del "conocimiento efectivo" puede hallarse no solamente en la notificación de la parte afectada, sino también en la forma e información que rodean la actividad de alojamiento o enlace. En el caso que nos ocupa, la Audiencia Provincial establece que no opera la exención de responsabilidad establecida en el art. 16, con base en que los contenidos son graves y no puede desconocer el representante legal de la demandada que, incluso sin valorarse en este ámbito, pudieran ser de ámbito penal. En segundo lugar, la parte demandada pudo razonablemente conocer el hilo de las conversaciones de

los usuarios, ya no solo por el largo periodo en que se han producido, sino por el consistente número de respuestas obtenidas.

Por tanto, partiendo de los hechos declarados probados por la Audiencia Provincial, la ilicitud de los materiales alojados es evidente por sí sola, no depende de datos o información que no se encuentran a disposición del intermediario, pues su ilegalidad es patente, por lo que conforme con la jurisprudencia el prestador de servicio no ha cumplido con el deber de diligencia a fin de detectar y prevenir determinados tipos de actividades ilegales. La conclusión alcanzada por la AP es plenamente conforme con la doctrina jurisprudencial fijada por esta Sala en lo relativo a la interpretación del art. 16 de la Ley 34/2002.»

Otro caso se plantea en la STS de 4 de marzo de 2013, en la que la demandada venía difundiendo textos en relación con la «trama de Roca», asunto relacionado con el sector inmobiliario en Marbella, y la «operación Malaya». Entendía la demandante que la información era falsa y carente de toda prueba y que tampoco se había empleado la más mínima diligencia profesional en la comprobación de los hechos. Se afirma además que la información permaneció colgada en Google a pesar de los requerimientos dirigidos a la demandada. La demanda se dirige contra Google y contra Don Ginés y se solicita una indemnización por daños morales de 100.000 euros.

En sus Fundamentos de Derecho, la sentencia se refiere a los servicios intermediarios en estos términos:

«En resumen, la normativa aplicable es la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, incorporando al ordenamiento español la Directiva 2000/31/CE y particularmente el art. 17 de dicho texto legal, y habiéndose acreditado la concurrencia de los requisitos que dicho artículo prevé para exonerar de responsabilidad a las empresas que prestan servicios de intermediación, dado que Google no tenía conocimiento de que la titular de la página PRNoticias había reconocido haber atentado contra el honor del demandante, siendo en este caso incluso innecesario la notificación a Google, puesto que cumpliéndose el acuerdo transaccional, la titular de la página retiraría la información lesiva, hecho que supondría la desaparición automática del enlace en el resultado de búsquedas en Google. Por otra parte y respecto a las otras dos publicaciones digitales, Telecinco y "Lobby per la Independencia", no consta resolución declarando la ilicitud de las publicaciones con lo cual no le era exigible a Google ninguna diligencia para retirar la información.

Conforme a lo expuesto, procede la desestimación de la demanda conforme al art. 17 LSSI al no ser la demandada Google Inc. ni Don Ginés responsables del contenido de los artículos publicados en la página de Telecinco de "Aquí hay Tomate" ni "Lobby per la Independencia" ni "PRnoticias" a los que se refiere la demanda.»

Se pueden citar otras sentencias sobre esta materia, entre ellas, la STS de 10 de febrero de 2011 o la STS de 4 de diciembre de 2012.

También la sentencia de la Audiencia Provincial (SAP) de Barcelona de 29 de octubre de 2014, que denegó la exención de responsabilidad a la Universidad Autónoma de Barcelona por los contenidos alojados en sus servidores que infringían derechos de propiedad intelectual y que habían sido subidos por profesores, al entender que se daba la relación de dependencia del artículo 16.2 LSSICE. Según este artículo, la exención de responsabilidad del artículo 16.1 (conocimiento efectivo), no se aplicará «en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador».

Un caso especialmente interesante y de gran actualidad es el «caso Uber», del cual, si bien todavía no hay sentencia, acaban de publicarse las conclusiones del abogado general sobre el caso. Considera que Uber no actúa como un intermediario de la sociedad de la información sino como un servicio de transporte:

«Conclusiones del Abogado General, Sr. Maciej Szpunar, presentadas el 11 de mayo de 2017 en el asunto C 434/15 (Asociación Profesional Élite Taxi): (Petición de decisión prejudicial planteada por el Juzgado de lo Mercantil n.º 3 de Barcelona).

Nota: El Abogado General propone al Tribunal que conteste las cuestiones planteadas en el siguiente sentido:

1) El artículo 2, letra a), de la Directiva 2000/3[1]/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), en relación con el artículo 1, apartado 2, de dicha Directiva y con el artículo 1, punto 2, de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, en su versión modificada por la Directiva 98/48/CE del Parlamento Europeo y del Consejo, de 20 de julio de 1998, debe interpretarse en el sentido de que un servicio consistente en conectar, mediante un software para teléfonos móviles, a pasajeros potenciales y a conductores que proponen prestaciones de transporte urbano individual a petición de aquellos, en una situación en la que el prestador de dicho servicio ejerce un control sobre las modalidades esenciales de las prestaciones de transportes llevadas a cabo en dicho marco, en particular sobre su precio, no es un servicio de la sociedad de la información en el sentido de dichas disposiciones.

2) El artículo 58 TFUE, apartado 1, y el artículo 2, apartado 2, letra d), de la Directiva 2006/123/CE, del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, deben interpretarse en el sentido de que el servicio descrito en el punto anterior constituye un servicio de transporte en el sentido de estas disposiciones.»

Se puede consultar el texto completo de las conclusiones en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=190593&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=681986.

4) Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. Igual que en el caso anterior, estos prestadores de servicios se exonerarán de responsabilidad por la información que dirijan a los destinatarios de sus servicios, siempre que:

- No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización.

- Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

No operará la exención, igual que en el supuesto anterior, cuando el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, la autoridad o el control del prestador que facilite la localización de esos contenidos.

Lectura recomendada

Sobre estos temas, se puede consultar el blog: https://responsabilidadinternet.wordpress.com/.

Para la reflexión

¿Quién es responsable de las opiniones vertidas en un foro? (Ver resoluciones de los Tribunales sobre esta cuestión).

Cuando se trata de prestadores de servicios intermediarios, ¿cuándo y de qué responden? Pensemos en un ejemplo, Airbnb: ¿hasta qué punto es responsable de una determinada oferta que no es lícita? O, ¿qué ocurre si se ha ofrecido una casa que no existe? ¿Y si los alojamientos no cumplen con la normativa de una determinada comunidad autónoma?

2. El prestador de servicios de la sociedad de la información y el responsable del tratamiento

Según la definición del Reglamento General de Protección de Datos, el responsable del tratamiento es la persona física o jurídica, la autoridad pública, los servicios u otro organismo que, solo o junto con otros, determine los fines o medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento o los criterios específicos para su nombramiento, podrá establecerlos el Derecho de la Unión o de los Estados miembros.

Por su parte, el artículo 3.d) de la LOPDP define **responsable del tratamiento** como: «toda persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, el contenido y el uso del tratamiento».

En el apartado anterior se han definido los prestadores de servicios de la sociedad de la información. Estos prestadores de servicios, en el ámbito de sus funciones, utilizarán datos de terceras personas. En estos casos, cuando los datos tengan la condición de datos de carácter personal, de acuerdo con las definiciones de la normativa aplicable descrita anteriormente, serán a su vez responsables del tratamiento, con las obligaciones que ello conlleva.

En aplicación de la LOPDP, para tratar estos datos será necesario, con carácter general, el consentimiento del destinatario, siempre que sea una persona física identificada o identificable. Como excepción, no será necesario este consentimiento, según el artículo 6.2 LOPDP, cuando los datos sean necesarios para el mantenimiento o cumplimiento del contrato.

Grimalt Servera afirma que, aunque en abstracto es difícil determinar qué datos son necesarios para la ejecución del contrato, en todo caso serían necesarios, cuando estemos ante un contrato oneroso, el nombre y los apellidos del destinatario, incluso el NIF, así como su dirección y también si es mayor de edad o no. Otros datos podrían resultar necesarios dependiendo de la naturaleza del tipo de servicio o la modalidad de pago.

Referencia bibliográfica

P. Grimalt Servera (2005). «Deberes y responsabilidades en materia de protección de datos». En: Cavanillas Múgica, S. (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares (págs. 170-171).

Para tratar datos de carácter personal será necesaria la obtención del consentimiento. De acuerdo con el artículo 5 del RGPD, los principios relativos al tratamiento exigen que los datos personales sean: tratados de manera lícita, leal y transparente en relación con el interesado; recogidos con fines determinados, explícitos y legítimos y que después no sean tratados de manera incom-

patible con dichos fines; adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; exactos y, si fuera necesario, actualizados.

El artículo 6 del RGPD establece que el tratamiento será lícito si cumple al menos una de las condiciones que enumera. En nuestro caso, nos interesa la primera: el consentimiento para el tratamiento de sus datos personales «para uno o varios fines específicos», y la segunda, «el tratamiento es necesario para la ejecución del contrato en el que el interesado es parte», y añade «o para la aplicación a petición de este de medidas precontractuales».

Se puede plantear si sería aplicable al ámbito de la mercadotecnia el apartado f) del artículo 6, que señala que el tratamiento será lícito «si es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y las libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño». Creemos que en el ámbito de la publicidad será más difícil de encajar, ya que para el tratamiento de datos para estos fines será necesario, con carácter general salvo excepciones, el consentimiento. En el caso de un sujeto que entra en una página web y se extrae información del mismo, se tendría que ver en cada caso el uso que se hace de esa información.

Lectura recomendada

Sobre la cuestión del interés legítimo, véase:

M. Vilasau Solana (2011). «Consentimiento, fuentes accesibles al público e interés legítimo como mecanismos que legitiman el tratamiento de datos de carácter personal». En: Blasco Gascó, F. y otros (coords.). *Estudios jurídicos en homenaje a Vicente L. Montés Penadés*, tomo II. Valencia: Tirant lo Blanch (págs. 2877-2898).

3. Interesado y consumidor

Hay que tener en cuenta tres conceptos: **destinatario del servicio de la sociedad de la información**, **afectado** o **interesado** –según terminología de la LOPDP– y **consumidor** –de acuerdo con el TRLGDCU.

El **destinatario de servicios** es la persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

Y el **afectado** o **interesado** es, según la LOPDP, «la persona física titular de los datos que sean objeto del tratamiento al que se refiere el apartado c) de este artículo». A estos efectos se entiende por **tratamiento de datos** las «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

El Reglamento General de Protección de Datos define **destinatario** como «la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento».

La definición de **destinatario de servicios de la sociedad de la información** es más amplia que la de **interesado** de la LOPDP, ya que el primer término incluye las personas jurídicas y el segundo, no. Solo en este último caso sería de aplicación la LOPDP o el Reglamento por lo que se refiere al tratamiento de datos personales.

La LSSICE en su Anexo también incluye una definición de **consumidor** y lo hace remitiendo a la definición establecida en la Ley General para la Defensa de los Consumidores y Usuarios, hoy Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios. Según su artículo 3, son consumidores y usuarios «las personas físicas o jurídicas que actúen en un ámbito ajeno a una actividad empresarial o profesional». Extiende, a diferencia de la Directiva europea, el concepto de **consumidor** también a las personas jurídicas. Según la Directiva 2011/83/UE[1], es consumidor «toda persona física que, en contratos regulados por la presente Directiva, actúe con un propósito ajeno a su actividad comercial, empresa, oficio o profesión». Como se ve, solo se

(1)Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo.

refiere a la persona física, a diferencia de la norma española. Si fuera así, en la norma española de transposición de la Directiva 2011/83 podría coincidir con el «interesado» de la LOPDP.

Hay que recordar que al «consumidor», además de lo establecido en la LSSICE, cuando sea persona física y en relación a la protección de sus datos de carácter personal, se le aplicarán las disposiciones de la LOPDP y el TRLGDCU, siendo especialmente importante aquello relativo a la oferta, promoción y publicidad, su carácter vinculante, etc.

Normativa autonómica

En el caso de la Ley 7/2014, de 23 de julio, de Protección de las Personas Consumidoras y Usuarias de las Illes Balears, se define a los **consumidores** como las personas físicas o jurídicas que actúen con un propósito ajeno a su actividad comercial, empresa, oficio o profesión. Al igual que han hecho otras comunidades autónomas, se ha introducido la figura del «consumidor especialmente vulnerable» que incluye, entre otros, a los menores.

Según la Ley 5/2013, de 12 de abril, para la defensa de los consumidores en la Comunidad Autónoma de La Rioja, «es consumidor toda persona física o jurídica que, actuando en un ámbito ajeno a su actividad profesional, adquiera, utilice o disfrute, como destinatario final, para uso o consumo personal, familiar o colectivo, bienes muebles o inmuebles, productos, servicios, actividades o funciones siempre que quien los ofrezca o ponga a su disposición ostente la condición de empresario o profesional, con independencia de su naturaleza pública o privada».

Y el Código de Consumo de Cataluña (aprobado por Ley 22/2010, de 20 de julio) define **consumidor medio**, término que no se encuentra en otras normas, entendiendo por tal la persona que, «de acuerdo con un criterio de diligencia ordinaria, debería estar normalmente informada y ser razonablemente cuidadosa en las relaciones de consumo, en función de los factores sociales, culturales y lingüísticos».

La Exposición de Motivos de la Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de los consumidores y usuarios, también se refiere al «consumidor medio», remitiendo a los tribunales para su consideración en cada caso concreto. Lo hace en estos términos:

> «El concepto de "consumidor medio" ha sido acuñado por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas no en términos estadísticos, sino como la reacción típica del consumidor normalmente informado, razonablemente atento y perspicaz, teniendo en cuenta los factores sociales, culturales y lingüísticos. En consecuencia, no es un término que la ley haya de definir, sino que han de ser los tribunales los que van a efectuar su concreción en cada caso concreto.»

A este consumidor y usuario hay que prestar especial atención cuando nos referimos a la calidad de la información facilitada con carácter previo al consentimiento, que es una constante en el ámbito de la publicidad y la protección de datos. A ello se refiere la «Guía para el uso de *cookies*» de la Agencia Española de Protección de Datos (AEPD) cuando menciona la calidad de la información que debe facilitarse para el uso de *cookies*:

«Tener en cuenta el tipo de usuario medio al que se dirige esa página web y adecuar el lenguaje y el contenido de los mensajes a su nivel técnico. Cuanto menor sea el nivel técnico del usuario medio de esa página web, más sencillo deberá ser el lenguaje que se utilice (evitando terminología técnica poco comprensible) y más completa la información que se ofrezca, partiendo de los aspectos más básicos de qué son las *cookies* y cómo funcionan. En todo caso, ese menor nivel técnico no deberá ser óbice para que la información facilitada sea lo más clara posible, evitando recargar la información con detalles innecesarios que hagan farragosa su lectura.»

«Guía para el uso de *cookies*» (disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf).

Más allá de nuestras fronteras, la propuesta normativa en la que confluyen la protección de los consumidores y la protección de la privacidad de los mismos es la Consumer Privacy Bill of Rights (disponible en: https://www.congress.gov/bill/114th-congress/senate-bill/1158/text) en EE.UU.

Lectura recomendada

Sobre la Consumer Privacy Bill of Rights, véase: https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/.

En relación a este proyecto normativo, afirma Díaz Díaz que «busca establecer un marco para la protección de la privacidad y la promoción de la innovación en la economía digital mundial, consciente de que representa un papel fundamental en el crecimiento económico sostenible y en el desarrollo de la propia sociedad del conocimiento». Según el estudio realizado por este autor, las principales compañías de Internet y las redes de publicidad en línea se comprometen a aplicar la tecnología del «*Do Not Track*» en la mayoría de los principales navegadores de Internet para facilitar a los usuarios el control del seguimiento en línea.

Referencia bibliográfica

E. Díaz Díaz (2016). «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones». *Revista Aranzadi Doctrinal* (núm. 6/2016. BIB 2016\3067).

Por otra parte, se trata de una norma que pretende proteger los derechos de los consumidores, de los cuales el propio Díaz Díaz apunta los siguientes:

«1) Control del individuo, pues los consumidores tienen derecho a ejercer el control sobre los datos personales que las organizaciones recogen de ellos y a conocer cómo los utilizan;

2) transparencia, ya que los consumidores tienen derecho a una información fácilmente comprensible sobre las prácticas de privacidad y seguridad;

3) respeto del contexto: los consumidores tienen derecho a que las organizaciones procedan a recopilar, utilizar y revelar datos personales de manera coherente con el contexto en el que los consumidores suministran los datos, sin destinarlos a finalidades distintas ni incompatibles;

4) seguridad: los consumidores tienen derecho a asegurar y manejar de forma responsable los datos personales en las plataformas tecnológicas puestas a disposición por las empresas (que deben evaluar los riesgos para la privacidad y la seguridad asociados con usos de datos personales y mantener salvaguardas razonables para controlar riesgos como la pérdida, el acceso no autorizado, el uso, la destrucción o modificación y la divulgación indebida);

5) acceso y exactitud: los consumidores tienen derecho a acceder a los datos personales correctos en formatos reutilizables, de una manera que sea apropiada a la sensibilidad de los datos y al riesgo de consecuencias adversas para los consumidores si los datos son inexactos;

6) *accountability*: los consumidores tienen derecho a que los datos personales sean tratados por las empresas con las medidas adecuadas para asegurarse de que se adhieren a la Ley en vigor.»

La mayoría de estos derechos se recogen en la normativa europea y española de protección de datos: el uso de los datos, con pleno conocimiento del usuario, las finalidades a las que se destinan los datos, la transparencia en relación con la información sobre las políticas de privacidad, etc. Son cuestiones que ya conocemos y que recoge nuestra normativa.

4. Comunicaciones comerciales por vía electrónica

4.1. Planteamiento y regulación

En el tema de las comunicaciones comerciales, se presentan dos bloques de intereses contrapuestos. Queda patente la contradicción entre los intereses de las empresas de marketing directo y los de los consumidores. La Propuesta de Reglamento define **mercadotecnia directa** como: «toda forma de publicidad oral o escrita enviada a uno o varios usuarios finales, identificados o identificables, de servicios de comunicaciones electrónicas, incluyendo la utilización de sistemas automatizados de llamada y comunicación con interacción humana o sin ella, correo electrónico, SMS, etc.»–; así, las empresas del este sector quieren hacer llegar su publicidad al mayor número posible de destinatarios, utilizando todas las vías a su alcance. Mientras que los consumidores o destinatarios de las mismas no quieren, en general, ver inundado su correo electrónico o su teléfono móvil con mensajes publicitarios u ofertas promocionales que no han solicitado, con los costes temporales y económicos que ello puede conllevar, además de plantearse, desde otra perspectiva, como una vulneración de su privacidad.

Comunicación comercial

La Resolución R/01312/201 de la AEPD (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_ sancionadores/ps_2017/common/pdfs/PS-00089-2017_Resolucion-de-fecha-19-05-2017_Art-ii-culo-21.1-LSSI.pdf) de la AEPD se refiere al concepto de *comunicación comercial*:

«Como ya se ha señalado, la LSSI prohíbe las comunicaciones comerciales no solicitadas o expresamente autorizadas, partiendo de un concepto de comunicación comercial que se califica como servicio de la sociedad de la información y que se define en su Anexo de la siguiente manera:

"f) 'Comunicación comercial': toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica."

El concepto de *comunicación comercial*, de acuerdo con la definición recogida en el Anexo f), párrafo primero de la LSSI, engloba todas las formas de comunicaciones destinadas a promocionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o profesional.»

En relación al concepto de **publicidad y comunicación comercial**, de Miguel Asensio afirma que:

«El concepto de comunicación comercial del apartado f) del Anexo LSSI –art. 2.f) DCE– favorece la superación de un elemento tradicionalmente asociado al término publicidad, pese a no estar expresamente incluido en la definición del artículo 2 LGP. Se trata de la idea de que la publicidad constituye comunicación colectiva, lo que había llevado a considerar en ocasiones que la comunicación dirigida a un solo destinatario no es propiamente publicidad. Ciertas actividades, como las llevadas a cabo mediante el correo electrónico (y postal), a través del envío de mensajes SMS y MMS o incluso por medio del contacto interactivo con los usuarios de sitios web, hacen posible la comunicación individualizada con el destinatario, aunque el desarrollo de la actividad publicitaria por esos medios aparece enmarcado normalmente en una actividad dirigida a una pluralidad de destinatarios. El concepto de comunicación comercial de la LSSI facilita la inclusión de ese tipo de comunicaciones, con independencia de que vayan dirigidas o no a una pluralidad de destinatarios. La circunstancia de que ciertos mecanismos de comunicación individual constituyen medios publicitarios de gran importancia en Internet aparece reflejada con claridad en los instrumentos de autorregulación en este ámbito. Así, el artículo 9 del Código Ético de Comercio Electrónico y Publicidad Interactiva de Confianza Online, aparece dedicado a la regulación de la "publicidad" mediante correo electrónico y otros medios de comunicación "individual" equivalentes.»

P. A. de Miguel Asensio (2015). «Prácticas desleales y comunicaciones comerciales». En: de Miguel Asensio, P. A. *Derecho Privado de Internet*. Cizur Menor: Westlaw (BIB 2015\7).

Consciente de la contraposición planteada, la regulación sobre la materia ha querido dejar plasmada aquella situación intentando buscar un equilibrio que se pretende alcanzar con una regla general: el sistema de listas positivas (conocido como *opt in*) para el envío de comunicaciones comerciales y, seguidamente, el establecimiento de una excepción para algunos supuestos específicos en donde las empresas podrán enviar comunicaciones comerciales sin que sea necesario obtener el consentimiento previo del destinatario.

El análisis de esta materia cobra especial interés por la confluencia de distintos aspectos y, a su vez, de distinta normativa para dar una solución a la cuestión planteada. En este punto de intersección se encuentra la normativa sobre comercio electrónico (LSSICE) y la relativa a la protección de datos de carácter personal (LOPDP).

Pero de igual modo hay que tener en cuenta el artículo 96 TRLGDCU, también sobre comunicaciones comerciales a distancia:

«1. En todas las comunicaciones comerciales a distancia deberá constar inequívocamente su carácter comercial.

2. En el caso de comunicaciones telefónicas, deberá precisarse explícita y claramente, al inicio de cualquier conversación con el consumidor y usuario, la identidad del empresario, o si procede, la identidad de la persona por cuenta de la cual efectúa la llamada, así como indicar la finalidad comercial de la misma. En ningún caso, las llamadas telefónicas se efectuarán antes de las 9 horas ni más tarde de las 21 horas, ni en festivos o fines de semana.

3. La utilización por parte del empresario de técnicas de comunicación que consistan en un sistema automatizado de llamadas sin intervención humana o el telefax necesitará el consentimiento expreso previo del consumidor y usuario.

El consumidor y usuario tendrá derecho a no recibir, sin su consentimiento, llamadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los referidos en el apartado anterior, cuando hubiera decidido no figurar en las guías de comunicaciones electrónicas disponibles al público, ejercido el derecho a que los datos que aparecen en ellas no sean utilizados con fines de publicidad o prospección comercial, o solicitado la incorporación a los ficheros comunes de exclusión de envío de comunicaciones comerciales regulados en la normativa de protección de datos personales.

4. El consumidor y usuario tendrá derecho a oponerse a recibir ofertas comerciales no deseadas, por teléfono, fax u otros medios de comunicación equivalente.

En el marco de una relación preexistente, el consumidor y usuario tendrá asimismo derecho a oponerse a recibir comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente. Debe ser informado en cada una de las comunicaciones comerciales de los medios sencillos y gratuitos para oponerse a recibirlas.

5. En aquellos casos en que una oferta comercial no deseada se realice por teléfono, las llamadas deberán llevarse a cabo desde un número de teléfono identificable. Cuando el usuario reciba la primera oferta comercial del emisor, deberá ser informado tanto de su derecho a manifestar su oposición a recibir nuevas ofertas como a obtener el número de referencia de dicha oposición. A solicitud del consumidor y usuario, el empresario estará obligado a facilitarle un justificante de haber manifestado su oposición que deberá remitirle en el plazo más breve posible y, en todo caso, en el plazo máximo de un mes.

El emisor estará obligado a conservar durante al menos un año los datos relativos a los usuarios que hayan ejercido su derecho a oponerse a recibir ofertas comerciales, junto con el número de referencia otorgado a cada uno de ellos, y deberá ponerlos a disposición de las autoridades competentes.

6. En todo caso, deberán cumplirse las disposiciones vigentes sobre protección de los menores y respeto a la intimidad. Cuando para la realización de comunicaciones comerciales se utilicen datos personales sin contar con el consentimiento del interesado, se proporcionará al destinatario la información que señala el artículo 30.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y se ofrecerá al destinatario la oportunidad de oponerse a la recepción de las mismas.»

La LSSICE ha optado claramente por el sistema de listas positivas para el caso de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente.

La mayor protección del destinatario de estas comunicaciones, junto a los problemas que derivan del sistema de listas negativas (la obligación de consultar las listas, el establecimiento del responsable de estas listas, la necesaria determinación de qué listas se deben consultar, la actualización de las mismas y el riesgo de que sean utilizadas ilícitamente), parece que quedan plasmados en la normativa mencionada. Pero, tanto en un caso como en otro, queda patente el cruce con las normas sobre protección de datos: el alcance de la noción misma de **dato de carácter personal** (dirección de correo electrónico, número de teléfono móvil), datos obtenidos de fuentes accesibles al público, etc.

Hay que tener en cuenta que toda esta cuestión está siendo objeto de reforma con la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, que sustituirá a la Directiva 2002/58/CE.

Como afirma la Propuesta de Reglamento, hay que proteger a los usuarios finales de las intromisiones que supone el envío de comunicaciones comerciales no solicitadas, sean del tipo que sean: sistemas automatizados de llamada, mensajería instantánea, correo electrónico, SMS, MMS, *bluetooth*, etc. Se establece la necesidad de consentimiento previo para el envío de estas comunicaciones con el fin de proteger a las personas de su intromisión en su vida privada y garantizar «los intereses legítimos de las personas jurídicas».

Por su parte, el Reglamento General de Protección de Datos define **datos personales** como:

> «[...] toda información sobre una persona física identificada o identificable ("el interesado"): se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.»

Y ya sabemos que la LOPDP define el **dato de carácter personal** como «cualquier información concerniente a personas físicas identificadas o identificables». Parece que la dirección de correo electrónico, siempre que pertenezca a una «persona física», sería un dato de carácter personal. La duda puede plantearse con aquellas direcciones en las que no se puede identificar a una persona en concreto.

Lo que hay que plantearse a continuación es si el número de teléfono móvil constituye, también, un dato de carácter personal. El Código de Conducta Europeo para el Uso de Datos Personales en el Marketing Directo (Federación Europea de Marketing Directo: https://www.fedma.org/) incluye expresamente en su definición de datos de carácter personal los números de teléfono y las direcciones de correo electrónico. Y el «Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE» del Grupo de Trabajo del Artículo 29 (disponible en http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_es.pdf) se refería al *e-mail*, a los mensajes SMS, al fax, al teléfono, etc., como comunicaciones electrónicas.

En principio, parece que puede entenderse como una información concerniente a una persona física –quedarían descartados, pues, los teléfonos móviles pertenecientes a empresas. Según el artículo 21 LSSICE, queda prohibido el envío de comunicaciones comerciales a través de correo electrónico «u otro medio de comunicación electrónica equivalente». Por otra parte, la «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o "spam"» (disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52004AR0069&from=ES), no deja lugar a dudas: incluye expresamente en la Directiva 2002/58/CE los mensajes SMS o MMS enviados a teléfonos móviles.

Pero lo establecido en estas normas tiene que llevarse a la práctica. Solo estableciendo un conjunto de medidas eficaces, la finalidad pretendida por las mismas obtendrá una respuesta. Estas medidas pasan necesariamente por aspectos técnicos (sistemas de filtrado y seguridad), códigos de conducta, mecanismos extrajudiciales de solución de conflictos, etc. Hay que conjugar medidas legales, medidas técnicas y políticas empresariales claramente destinadas a evitar el conocido *spam*.

4.2. Regla general: el sistema *opt in*

Si bien la normativa sobre contratos a distancia, en un tímido acercamiento al sistema de listas positivas, las exigía para el caso del sistema automático de llamadas o fax, es con la LSSICE cuando se opta claramente por este sistema en el caso del envío de comunicaciones comerciales no solicitadas a través del correo electrónico, sistema que corroboró la Directiva sobre privacidad y comunicaciones electrónicas –ahora en revisión–, por lo que la opción por este sistema debería quedar garantizada en el ámbito europeo, lo que supone, además, una garantía para el consumidor. Para el análisis de esta cuestión, también debe tenerse en cuenta el artículo 48 de la Ley General de Telecomunicaciones (LGT).

El artículo 13 de la Directiva sobre privacidad y comunicaciones electrónicas, en relación a las comunicaciones no solicitadas, establece que:

> «1. Solo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.
>
> 2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.
>
> 3. Los Estados miembros tomarán las medidas adecuadas para garantizar que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional.
>
> 4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.
>
> 5. Los apartados 1 y 3 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a las comunicaciones no solicitadas.»

Aquí se definen los sistemas *opt in* y *opt out*.

Según el artículo 48 de la Ley General de Telecomunicaciones («Derecho a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, con los datos de tráfico y de localización y con las guías de abonados»):

«1. Respecto a la protección de datos personales y la privacidad en relación con las comunicaciones no solicitadas, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos:

a) A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de comunicación comercial sin haber prestado su consentimiento previo e informado para ello.

b) A oponerse a recibir llamadas no deseadas con fines de comunicación comercial que se efectúen mediante sistemas distintos de los establecidos en la letra anterior y a ser informados de este derecho.»

Como ha quedado expuesto, hace falta consentimiento previo, el cual, según la LOPDP, será una manifestación de voluntad libre, inequívoca, específica e informada, y de acuerdo con el artículo 7 del Anteproyecto de LOPDP: «toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen», evitando con la mención a «una clara acción afirmativa» el consentimiento tácito. Aunque en este caso hay que distinguir la necesidad de consentimiento para enviar una comunicación comercial y el tratamiento de datos de carácter personal, que también requerirá consentimiento, pero hay casos en los que se establece una excepción.

Algunas resoluciones de la AEPD sobre esta cuestión

1) AEPD: «Expediente Nº: E/02202/2016. Resolución de archivo de actuaciones» (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2017/common/pdfs/E-02202-2016_Resolucion-de-fecha-16-01-2017_Art-ii-culo-13-6-LOPD.pdf).

Se plantea la posibilidad de que se estén recogiendo datos sin cumplir los requisitos legales. Se afirma que hay una recopilación extensa de datos para la concesión de un crédito. Estos datos llegan a:

«Si es posible, el algoritmo incluso explora la cronología de Facebook del solicitante, que es un espacio privado en las redes sociales para comunicarse entre amigos y allegados. Aunque este componente solo se usa si existe el consentimiento específico del solicitante, KREDITECH no pide a otros usuarios de Facebook su consentimiento, a pesar de que sus datos también se recopilan con este método. A parte de eso, cabe dudar de que el consentimiento del solicitante se haya otorgado voluntariamente. En primer lugar, el potencial deudor podría ser recompensado por compartir sus datos de Facebook o al menos se le ofrece un tratamiento preferencial. En segundo lugar, los solicitantes que son rechazados, sin dar su consentimiento a la recopilación de datos de las redes sociales, probablemente se ven forzados a ofrecer dicha información al ser KREDITECH el único medio a su alcance para pedir prestado dinero.

Además, es obligatorio para los solicitantes indicar la contraseña de sus cuentas bancarias en Internet para permitir al programa examinar todas las transacciones producidas en los últimos sesenta días.

En resumen, el algoritmo automatizado obtiene un conocimiento amplio y profundo del entorno del solicitante. Teniendo en cuenta que KREDITECH también posee calificaciones de agencias de solicitud de crédito externas y que los deudores potenciales solo solicitan pequeños importes de crédito, consideramos que la recopilación extensa de datos es desproporcionada.»

A partir de aquí se analizan los hechos planteados y se plantea, entre otros aspectos, si los datos se recogen con el consentimiento de los interesados y si se ha obtenido este consentimiento de forma válida. Entiende la AEPD que la empresa en cuestión actúa con el consentimiento de sus clientes y que la finalidad es la de formalizar una relación contractual, en este caso, un préstamo.

2) AEPD: «Resolución R/02897/2015. Procedimiento sancionador PS/00280/2015 a la entidad TEKOA CANAL

TV S.L» (disponible en http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00280-2015_Resolucion-de-fecha-12-11-2015_Art-ii-culo-21-LSSI.pdf).

Constan como hechos probados que se enviaron SMS (concretamente, 29 SMS con contenido comercial) por la empresa TEKOA, sin quedar acreditada la existencia de consentimiento, ni relación contractual previa, además de no ofrecer un sistema de oposición para solicitar la baja del envío de comunicaciones electrónicas.

Sobre el artículo 21 y la necesidad de consentimiento previo del destinatario, afirma que:

«[...] la LSSI, en su artículo 21.1 prohíbe de forma expresa las comunicaciones comerciales dirigidas a la promoción directa o indirecta de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, sin consentimiento expreso del destinatario, si bien esta prohibición encuentra su excepción en el segundo párrafo del citado artículo, que autoriza el envío cuando "exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente". De este modo, el envío de comunicaciones comerciales no solicitadas, fuera del supuesto excepcional del artículo 21.2 de la LSSI, puede constituir una infracción leve o grave de la LSSI.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre, introdujo en el conjunto de la Unión Europea el principio de "*opt in*", es decir, la necesidad de contar con el consentimiento previo del destinatario para el envío de comunicaciones electrónicas con fines comerciales. De este modo, cualquier envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente queda supeditado a la prestación previa del consentimiento, salvo que exista una relación contractual anterior y el sujeto no manifieste su voluntad en contra.

El artículo 19, apartado 2, de la LSSI preceptúa que "En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y el mantenimiento de ficheros de datos personales".

Por tanto, en relación con el consentimiento del destinatario para el tratamiento de sus datos con la finalidad de enviarle comunicaciones comerciales por vía electrónica, es preciso considerar lo dispuesto en la normativa de protección de datos y, en concreto, en el artículo 3.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD) que define el "consentimiento del interesado" como: "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".

Asimismo resulta aplicable lo previsto en el artículo 45.1.b) del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que señala que cuando los datos se destinen a publicidad y prospección comercial, los interesados a quienes se les solicite su consentimiento deberán ser informados "sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad".»

Todo ello se plasma en el artículo 16 de la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas.

Las personas físicas o jurídicas podrán utilizar servicios de comunicaciones electrónicas para el envío de comunicaciones de mercadotecnia directa a los usuarios finales que sean personas físicas y hayan dado su consentimiento. La propuesta define **comunicaciones de mercadotecnia directa** como «to-

da forma de publicidad oral o escrita enviada a uno o varios usuarios finales identificados o identificables de servicios de comunicaciones electrónicas, incluyendo la utilización de sistemas automatizados de llamada y comunicación con interacción humana o sin ella, correo electrónico, SMS, etc.».

Nota

Es interesante lo que afirma la «Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)» del Grupo de Trabajo del Artículo 29:

«[...] the scope of direct marketing is too limited. In Art. 4(3) (f) of the Proposed Regulation, "direct marketing communications" are defined as "any form of advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services". The use of the word "sent" implies the use of technological communication means that necessarily involve the conveyance of a communication, whereas most advertising on the web (through social media platforms or on websites) would not involve "sending" advertisements in the strict sense. This is further underlined by the examples which follow in this definition (SMS, email) and in recital 33. These all refer to quite traditional forms of marketing communication, and even then the use of – quite traditional – calling systems arguably does not fall within the scope. The Article and recital should be amended to include all advertising sent, directed or presented to one or more identified or identifiable end-users. In addition, it should further be ensured that behavioural advertisements (based on the profiles of end-users) are also considered direct marketing communications directed at "one or more identified or identifiable end-users" (as such advertisements are targeted to specific, identifiable users).

Further, under the proposed scope of "direct marketing communications", the protection of Art. 16(1) would be limited to messages containing advertising material, and would not protect individuals from other messages sent, directed or presented for marketing purposes (such as lead-generation messages seeking consent, promotion of political views or voting preferences, promotion of charities or other non-profit organisations or general branding of an organisation). Moreover, fax machines are still in use as a direct marketing method, although they are not mentioned in the definition. Article 4(3)(f) should therefore include any form of advertising, canvassing or promotion, also for non-profit organisations, and should explicitly include fax machines alongside email and SMS (see also the suggestion for clarification in remark 43(a). Lastly, recital 32 states that direct marketing includes messages sent by political parties to promote their parties. This should be updated to include politicians and candidates for election who are promoting their candidacy.»

Se puede consultar este documento en: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Cuando se utilicen llamadas de mercadotecnia directa, se deben cumplir los siguientes requisitos:

- Presentar la identificación de una línea en la que se les pueda contactar.
- Presentar un código o prefijo específico que permita identificar que se trata de una llamada de mercadotecnia.

Los Estados miembros podrán establecer que la realización de llamadas de voz a voz, con fines de mercadotecnia directa, a usuarios finales que sean personas físicas solo quede autorizada con respecto a los usuarios finales que sean personas físicas y no hayan manifestado su oposición a recibir tales comunicaciones.

Por lo que se refiere a las personas jurídicas, los Estados miembros velarán para que el interés legítimo de los usuarios finales que sean personas jurídicas esté suficientemente protegido en lo que se refiere a las comunicaciones no solicitadas enviadas a través de servicios de comunicaciones electrónicas.

Nota

Sobre esta cuestión, la «Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)» (disponible en: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083) afirma que:

«The application of the direct marketing rules to legal persons. Art. 16(5) of the Proposed Regulation provides that Member States shall ensure the legitimate interest of end-users that are legal persons with regard to unsolicited communications are sufficiently protected. Art. 13(5) of the current ePrivacy Directive describes the legitimate interests of subscribers other than natural persons. It is unclear what the implications of this change in wording are. It should be clarified in the recitals that this change does not reflect the intention to provide a lower level of protection. In relation to this, the prohibition on direct marketing without consent relates to "end-users who are natural persons that have given their consent" (emphasis added). It should be clarified that this includes natural persons working for legal persons. On the other hand, consent would not be required to approach legal persons through generic contact details they have made public for this purpose (such as 'info@companyname.eu').»

Quien utilice servicios de comunicaciones electrónicas para comunicaciones de mercadotecnia directa tiene que informar:

- del carácter comercial de la comunicación,
- de la identidad de la persona física o jurídica en nombre de la cual se transmite la comunicación y
- tendrá que proporcionar la información necesaria a los destinatarios para que puedan ejercer fácilmente su derecho a retirar el consentimiento para no recibir nuevas comunicaciones de mercadotecnia.

Se otorgarán poderes a la Comisión para que pueda especificar el código o prefijo que ha de utilizarse para identificar las llamadas de mercadotecnia.

La pregunta que surge inmediatamente es: ¿qué ocurre cuando un país con el sistema de listas negativas envía comunicaciones comerciales no solicitadas a un consumidor de un país que no lo permite? Cuestión especialmente delicada cuando en EE.UU. se ha optado por un sistema más flexible. En este caso, entraríamos en un tema de Derecho internacional privado para determinar la ley aplicable a estos casos.

La *Can Spam Act* de 2003

La normativa de EE.UU. sobre esta materia es la *Can Spam Act* de 2003. En el caso del correo electrónico, se basa en el sistema *opt out*: el correo electrónico no solicitado debe estar claramente identificado, debe incluir un sistema fácil y accesible para que el destinatario pueda oponerse a recibir más mensajes que contenga un sistema de retorno y la dirección física de quien lo envía. Se considera ilícito enviar correos electrónicos a direcciones obtenidas de listas en Internet.

Sin embargo, esta norma establece un régimen específico para el caso del envío de mensajes SMS: no se pueden enviar mensajes de texto SMS a menos que haya autorización ex-

presa con alguna excepción. Aún en el caso de la excepción, se debe permitir al destinatario que pueda indicar su deseo de no recibir más mensajes publicitarios o comerciales.

En la *Can Spam Act* 2003 de EE.UU. se define la expresión *transactional or relationship message* como:

«[...] an electronic mail message the primary purpose of which is: (i) to facilitate, complete, or confirm a commercial transaction that the recipient has previously agreed to enter into with the sender; (ii) to provide warranty information, product recall information, or safety or security information with respect to a commercial product or service used or purchased by the recipient; (iii) to provide. (I) notification concerning a change in the terms or features of; (II) notification of a change in the recipient's standing or status with respect to, a subscription membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of products or services offered by the sender; (iv) to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating or enrolled; or (v) to deliver goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender.»

Sobre esta cuestión, es interesante el artículo «CAN-SPAM Act: A Compliance Guide for Business», disponible en: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

4.3. La excepción al sistema *opt in*: el artículo 21.2 LSSICE

La regla general de la necesidad de consentimiento previo para el envío de comunicaciones comerciales encuentra una excepción en el apartado segundo del artículo 21 LSSICE. Según este artículo, no hace falta el consentimiento previo si:

- Existe una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario.

- Estos datos los empleara para el envío de comunicaciones comerciales referentes a productos o servicios similares a los que inicialmente fueron objeto de contratación con el cliente.

- Y que sean productos o servicios de su propia empresa.

El antecedente normativo de la excepción se encuentra en el artículo 13.2 de la Directiva sobre la privacidad y las comunicaciones electrónicas. Esta norma establece el sistema de listas positivas para el envío de comunicaciones comerciales no solicitadas, con una excepción siempre que se den las siguientes circunstancias: una persona física o jurídica obtiene de sus clientes la dirección de correo electrónico; en el marco de la venta de un producto o servicio, de conformidad con lo establecido en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (como establece el artículo 6, los datos serán recogidos con fines determinados y no pueden ser tratados posteriormente de manera incompatible con dichos fines; según el artículo 7 se requiere el consentimiento del interesado, salvo en algunos supuestos determinados); la persona que ha recogido la dirección de correo electrónico podrá utilizarla para la venta directa de sus propios productos o servicios –no los de un tercero– de características similares. Y todo ello con la condición de que se

ofrezca al cliente la posibilidad de oponerse a esta utilización de su dirección de correo electrónico, en el momento en que se recoge o en un momento posterior (el artículo 14 de la Directiva 95/46/CE establece el derecho de oposición a la utilización de los datos del propio interesado).

La Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas mantiene, por entenderlo razonable, la autorización del uso de los datos de correo electrónico en el contexto de una relación preexistente con el cliente para ofrecerle productos o servicios similares. Eso sí, entiende que esta posibilidad solo debería aplicarse a la «misma empresa» que haya obtenido los datos de contacto electrónicos, de conformidad con el Reglamento General de Protección de Datos.

Según el artículo 16 de la Propuesta de Reglamento, cuando una persona física o jurídica obtenga los datos de contacto electrónicos de un cliente dentro de la venta de un producto o servicio, dicha persona únicamente podrá utilizar esos datos de contacto para la comercialización directa de sus propios productos o servicios similares cuando ofrezca al cliente, de manera clara y precisa, la oportunidad de oponerse a esa utilización de forma sencilla y gratuita. Este derecho de oposición se concederá en el momento de la recopilación y cada vez que se envíe un mensaje.

Planteado prácticamente sin discusión el sistema *opt in* para el caso del envío de comunicaciones comerciales no solicitadas, las dudas surgen en torno a la excepción del artículo 21.2 LSSICE: ¿cómo debe interpretarse? ¿Qué hay que entender por **relación contractual previa**? ¿Qué hay que entender por **productos o servicios similares a los que inicialmente fueron objeto de contratación con el cliente**? ¿Y por la **misma empresa**?

Para interpretar la excepción debe tenerse en cuenta que se trata precisamente de esto, de una excepción al régimen general establecido en aquella Ley, basado en la necesidad de consentimiento previo para poder enviar comunicaciones comerciales a través de correo electrónico. En el mismo sentido, el «Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_es.pdf), establece que la citada excepción –en este caso, refiriéndose a la Directiva sobre la privacidad y las comunicaciones electrónicas– debe interpretarse de modo restrictivo.

La configuración de la cuestión en otros países resulta especialmente interesante, pues las empresas de marketing directo pueden verse favorecidas según se encuentren en un lugar o en otro, dependiendo de su normativa, y obviamente estarán mucho más cómodas donde la regulación sea más permisiva. La armonización en estas cuestiones es fundamental.

En la resolución de la AEPD 252/2005 se sanciona a una empresa de seguros por una infracción leve del artículo 21 LSSICE. Afirma dicha resolución que: «El envío de mensajes publicitarios o promocionales por correo electrónico debe haberse solicitado o autorizado expresamente por los destinatarios de los mismos, salvo que, existiendo una relación contractual previa, se trate de comunicaciones comerciales referentes a productos o servicios de la propia empresa que sean similares a los que inicialmente hubiesen sido objeto de contratación». La sanción se impone de acuerdo con lo establecido en la LSSICE (artículos 38.3 y 4 LSSICE).

4.3.1. Situación: relación contractual previa

El ámbito de la excepción queda delimitado con la existencia de una relación contractual previa, de forma muy similar a la Directiva sobre la privacidad y las comunicaciones electrónicas: los datos tenían que haberse obtenido en el contexto de la venta de un producto o servicio, de conformidad con la Directiva 95/46/CE.

Parece, tanto en un caso como en otro, que tiene que haberse perfeccionado un contrato entre las partes para que entre en juego la excepción. La solicitud de información sobre productos sin haber llegado a contratar, ¿se entiende ya como relación contractual previa? Parece que, en todo caso, sería una relación previa y no bastaría para aplicar el artículo 21.2 LSSICE. Todo ello parece corroborarse con el artículo 6.2 LOPDP, que establece que no será preciso el consentimiento cuando los datos de carácter personal se refieran a las partes de un «contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento».

Sin embargo, hay otras cuestiones problemáticas relacionadas con el tiempo y el modo, respectivamente, de esta «relación contractual previa»: ¿puede tratarse de un contrato celebrado hace mucho tiempo? ¿Dónde está el límite temporal? Y, por otra parte, ¿tiene que ser necesariamente una venta celebrada a través de medios electrónicos o puede haberse llevado a cabo con presencia física siempre que se hayan obtenido estos datos? La ley en este caso no distingue, se trata de un contrato previo, cualquiera que sea la forma en que se haya celebrado.

4.3.2. Forma: datos obtenidos de «forma lícita»

La Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, cuando habla en su artículo 16.2 de la excepción que venimos comentando, se refiere a la obtención de datos de su «cliente» en el contexto de la venta de un producto o servicio, de acuerdo con lo que establece el Reglamento General de Protección de Datos. Cumpliendo con ello, se habrían obtenido los datos de forma «lícita».

Ya ha quedado expuesto que tanto la dirección de correo electrónico como el número de teléfono móvil se consideran datos de carácter personal. Partiendo de la citada premisa, resulta especialmente interesante el cruce entre el artículo 30 LOPDP y el artículo 21.2 LSSICE.

El artículo 30 LOPDP es el que se dedica al tratamiento de datos con fines de venta directa estableciendo que, quienes se dediquen a la venta a distancia, prospección comercial y otras actividades análogas, «utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su propio consentimiento». Por su parte, el artículo 31 LOPDP establece que quienes se dedican a la venta a distancia, prospección comercial u otras actividades análogas podrán solicitar una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

Parece que en el censo promocional no se incluyen las direcciones de correo electrónico; entonces, las empresas de marketing directo no conseguirán por esa vía la dirección de correo electrónico o el número de teléfono móvil. Nos queda la dicción literal del artículo 30 en «otras fuentes accesibles al público» o bien, claro está, que se haya obtenido el consentimiento del cliente o consumidor. El problema que se plantea es si todo ello puede aplicarse al correo electrónico, al ser la LSSICE una norma posterior y establecer un régimen específico. Parece que por esta vía se cierran puertas para las empresas de marketing directo que quieren enviar por correo electrónico sus ofertas publicitarias.

Otra vía para conseguir los datos de carácter personal, aunque no medie el consentimiento del destinatario, es que los datos provengan de una relación contractual previa y se vayan a utilizar para las finalidades concretas que establece el artículo 21.2 LSSICE. A ello se une la prohibición del artículo 4.2 LOPDP de que los datos de carácter personal no podrán usarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos. Y el artículo 5 del RGPD, relativo a los principios, establece que los datos personales serán recogidos con fines determinados, explícitos y legítimos y no serán tratados para fines incompatibles, no considerándose incompatibles el posterior tratamiento de los datos con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

Por supuesto, si media consentimiento, ya no hay ningún problema para el tratamiento de estos datos, pero sí que se plantea una cuestión interesante respecto a la forma en que debe prestarse este consentimiento: es el caso de que se incluyera en un clausulado de condiciones generales. Según la LOPDP, el consentimiento del interesado se define como «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen». Y según el artículo 4 del RGPD, «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una decla-

ración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen». En cuanto a esta «manifestación de voluntad libre, inequívoca, específica e informada», lo que tendría que analizarse, caso por caso, es si la aceptación de un clausulado de condiciones generales es suficiente o cumpliría los requisitos exigidos por la Ley.

Sobre esta cuestión hay que tener en cuenta lo que dice el artículo 15 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 protección de datos de carácter personal:

> «Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o a la comunicación de datos. 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 relación con la licitud del consentimiento, otro tema interesante a tener en cuenta es el de los servicios gratuitos. En la resolución AEPD 442/2004 se trataba el caso de una asociación de consumidores que denunciaba el tratamiento de los datos de los usuarios del servicio de correo electrónico Gmail para el envío de publicidad no solicitada que se justificaba en la siguiente cláusula: «El usuario acepta que se pueda instalar software gratuito para el usuario a cambio de anuncios publicitarios. Estos anuncios en los que se basa la gratuidad del software podrán ser mostrados en su ordenador en cualquier tiempo o periodo de tiempo». La AEPD (resolución 1544/2007) entiende que en este caso el usuario presta el consentimiento expreso para el tratamiento de sus datos personales y para la asociación de publicidad personalizada, ya que es la contrapartida para la prestación gratuita del servicio.

Lectura recomendada

Sobre esta cuestión, véase:
A. Paniza Fullana (2009). «Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores». *Revista Española de Protección de Datos* (núm. 6, págs. 41-68).

4.3.3. Objeto: productos o servicios similares a los que inicialmente fueron objeto de contratación con el cliente

Se exige que los datos se hayan obtenido en una relación contractual previa y se utilicen para publicitar «productos o servicios similares». La Directiva sobre la privacidad y las comunicaciones electrónicas se refiere a «sus propios productos de características similares». No valdría cualquier producto de la misma marca, sino productos o servicios (de características) similares. Lo que nos conduce al tema de las finalidades incompatibles para el uso de los datos de carácter personal del artículo 4.2 LOPDP y el artículo 6.4 del Reglamento General de Protección de Datos. De nuevo, las normas se cruzan. En el «Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa», se establece que este no es un concepto fácil de aplicar en la práctica y debe enfocarse desde la perspectiva del destinatario, no desde la del vendedor. Debe tenerse en cuenta lo que razonablemente puede esperar el destinatario.

4.3.4. Sujeto: la misma empresa

Según el artículo 21.2 LSSICE, es necesario que los datos los utilice la «misma empresa». El artículo 13.2 de la Directiva sobre la privacidad y las comunicaciones electrónicas se refiere a una «persona física o jurídica» y que después sea esa misma «persona física o jurídica», no un tercero, quien utilice los datos.

¿Qué ocurre cuando se trata de un grupo de empresas? ¿Quién puede utilizar los datos recogidos en el marco de una relación contractual? Parece que, en principio, sería la que realmente ha sido parte en ese contrato. Por esta interpretación restrictiva parece decantarse el «Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa»: «*subsidiaries or mother companies are not the same company*». Y también la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas cuando en su artículo 16 establece (las negritas son nuestras):

Lectura recomendada

Sobre esta cuestión, véase:
«Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE» del Grupo de Trabajo del Artículo 29. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp90_es.pdf.

> «Cuando una persona física o jurídica obtenga los datos de contacto electrónicos de su cliente en el contexto de la venta de un producto o servicio, de conformidad con el Reglamento (UE) 2016/679, **dicha persona física o jurídica** solo podrá utilizar esos datos de contacto para la **comercialización directa de sus propios productos o servicios similares** cuando [...].»

Un ejemplo que encaja en este punto es el caso del operador de telefonía móvil que lanza sus propias ofertas: parece que este supuesto encaja en la excepción del artículo 21.2 LSSICE, es decir, relación contractual previa, datos obtenidos lícitamente, productos o servicios similares de su propia empresa. Aunque no se puede olvidar que siempre tiene que establecerse un procedimiento sencillo y gratuito de oposición.

4.3.5. Garantía: procedimiento sencillo y gratuito de oposición

Son constantes en la normativa las referencias a las medidas de oposición a la recolección de datos, incluso en los supuestos excepcionales que se vienen comentando.

Es el caso del artículo 21.2, párrafo segundo LSSICE:

> «En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.»

Y el de los artículos 30.4 y 31.3 LOPDP:

> «**Artículo 30.4**
>
> Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquel a su simple solicitud.»

«**Artículo 31.3**

Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y el domicilio de los que así lo hayan solicitado.»

En la práctica, algunas empresas lo que hacen es solicitar el envío de un escrito a la dirección física de la empresa, o piden que se llame a un teléfono gratuito o que se entre en una determinada página web. ¿Cumplen estas fórmulas con los requisitos del procedimiento «sencillo y gratuito» al que se refiere la Ley? La Comunicación de la Comisión Europea sobre las comunicaciones comerciales no solicitadas o *spam* establece que el régimen sobre comunicaciones comerciales tiene como norma fundamental el que todos los mensajes electrónicos deben mencionar una dirección de respuesta válida donde el abonado pueda pedir que no se le envíen más mensajes. Los aspectos legales y técnicos del tema confluyen necesariamente; una actuación conjunta aportaría soluciones eficaces.

Además, en el plano temporal, este procedimiento sencillo y gratuito de oposición debe ofrecerse tanto «en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija». Si bien en el caso del correo electrónico es bastante factible, la cuestión que se plantea es: ¿se cumple esto en los mensajes SMS? Con carácter general, no. ¿Podría suponer esta exigencia una carga demasiado elevada para la empresa en cuestión? ¿Qué vías técnicas pueden proponerse para que la aplicación real de esta normativa sea un hecho?

Por lo que se refiere al derecho de oposición, hay que tener en cuenta su regulación en el artículo 21 del RGPD y, concretamente en su apartado segundo, que se refiere al tratamiento de datos personales en el caso de mercadotecnia directa. En este caso, el interesado tendrá derecho a oponerse en todo momento al tratamiento de datos que le conciernan, incluyendo también la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Cuando el interesado se oponga a este tratamiento, sus datos dejarán de ser tratados para estos fines. Por lo que se refiere al plano temporal, como muy tarde en la primera comunicación al interesado, tiene que mencionarse expresamente el derecho de oposición y tiene que presentarse claramente y al margen de cualquier otra información. Según el artículo 21.5, en el contexto de la utilización de servicios de la sociedad de la información, «el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas».

4.4. Infracciones y sanciones

Enviar masivamente comunicaciones comerciales no solicitadas o su envío insistente o sistemático a un mismo destinatario del servicio, contraviniendo las reglas expuestas en el artículo 21, constituye infracción grave, según el artículo 38.3 b) LSSICE, y según el artículo 38.4 d) podrá tratarse, cuando no constituya una infracción grave, de una infracción leve. Todo ello se traduce en una multa de 30.001 a 150.000 euros en el primer caso, y de una de hasta 30.000 euros en el segundo.

Además, teniendo en cuenta que tanto la dirección de correo electrónico como el número de teléfono móvil se han considerado datos de carácter personal y, tal como se ha establecido, el envío de comunicaciones comerciales no solicitadas supone un ataque a la intimidad del destinatario, también puede suponer una infracción de la LOPDP por la utilización de datos personales sin el consentimiento del usuario –fuera de los casos en que la LOPDP lo permite–. Según el artículo 44.2 LSSICE, puede haber una doble infracción si resulta tipificada en otra Ley, siempre que no haya identidad del bien jurídico protegido. Con ello se plantean una serie de cuestiones: ¿se están protegiendo intereses distintos? ¿Supondría una doble infracción? ¿O se aplicaría la LSSICE por ser más específica? Parece que, en los supuestos que aquí se plantean, la LSSICE es más específica y el bien jurídico protegido muy similar. Es por ello por lo que la infracción aplicable es la que establece esta Ley. Además, en ambos casos, la imposición de sanciones corresponde a la Agencia de Protección de Datos.

Ejemplo

Resolución 177/2009 de la AEPD:

«El presente supuesto se ajusta al tipo de infracción establecido en el artículo 38.4.d) de la LSSI, calificado como infracción leve, al tratarse del envío por correo electrónico de una comunicación comercial a un mismo destinatario, sin consentimiento del mismo y sin ofrecerle un procedimiento para que pueda oponerse al tratamiento de sus datos con fines promocionales.»

Recapitulación

El envío de comunicaciones comerciales no solicitadas debe quedar restringido: es necesario el consentimiento previo por parte del destinatario, tanto en el caso en el que el medio utilizado sea el correo electrónico como en el que sean mensajes a través de teléfonos móviles. La normativa española ha optado por el sistema de listas positivas como norma general.

Este sistema de listas positivas que, como regla general, adopta la normativa española tiene una excepción para el caso de que exista una relación contractual previa entre las partes en unas circunstancias concretas. La ambigüedad e imprecisión de la excepción son sus notas características. Sin embargo, no puede olvidarse en ningún momento que debe interpretarse como tal, como una excepción, y que tal excepción no puede desvirtuar la finalidad de la ley. Una interpretación demasiado amplia del párrafo segundo del artículo 21 LSSICE provocaría esta desvirtuación.

A efectos prácticos, ¿qué posibilidades hay de que una empresa envíe mensajes de correo electrónico o SMS con fines publicitarios sin vulnerar los derechos del destinatario? En primer lugar, que la dirección de correo electrónico o los números de teléfonos móviles aparecieran en lo que la LOPDP denomina «fuente accesible al pú-

blico» (por ejemplo, una guía). En el caso de las guías, hay que tener en cuenta lo establecido en el artículo 48.3 de la Ley General de Telecomunicaciones:

«Respecto a la protección de datos personales y la privacidad en relación con las guías de abonados, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos: a) A figurar en las guías de abonados. b) A ser informados gratuitamente de la inclusión de sus datos en las guías, así como de la finalidad de las mismas, con carácter previo a dicha inclusión. c) A no figurar en las guías o a solicitar la omisión de algunos de sus datos, en la medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor.»

Si fuera así, según los artículos 5.5, 30 y 31 LOPDP, se podrían usar para fines publicitarios o de prospección comercial (difícilmente estos datos encajarán en la figura del censo promocional ya que este incluiría, según el artículo 31 LOPDP, los datos de nombre, apellidos y domicilio que constan en el censo electoral, pero no correo electrónico o número de teléfono móvil). Sin embargo, esta solución resulta muy discutible, como ya se ha explicado. Si no se da el supuesto expuesto anteriormente, hará falta el consentimiento del destinatario para el envío de estas comunicaciones comerciales o publicitarias. Y si no hay consentimiento y existe una relación contractual previa entre ambas partes, cabría la aplicación de la excepción contenida en el artículo 21.2 LSSICE, con los límites que la misma impone.

De la excepción puede extraerse lo siguiente:

- «Relación contractual previa»: no bastan meros tratos preliminares o una solicitud de información.
- Datos obtenidos de «forma lícita»: con el consentimiento e información suficiente al interesado.
- «Productos o servicios similares»: lo que razonablemente puede esperar el destinatario.
- «La misma empresa»: si hay que tratar el artículo 21.2 LSSICE como lo que verdaderamente es, una excepción, la misma empresa debería ser aquella con la que se ha celebrado el contrato, evitando así otras empresas de un mismo grupo, etc.
- La necesidad de establecer un procedimiento sencillo y gratuito de oposición: deben ser medidas que realmente tenga a su alcance cualquier consumidor sin que le supongan ningún gasto adicional.

La Comisión Europea propuso una serie de acciones tanto desde la perspectiva de los proveedores de servicios, que deberían ofrecer a los clientes información sobre filtros y programas o un servicio de filtrado, como de las empresas de venta directa, que deberían ponerse de acuerdo sobre métodos específicos conformes a la legislación de protección de datos personales, aprobar códigos de conducta y difundir las buenas prácticas de comercialización. Irremediablemente, las medidas tecnológicas avanzan de forma más rápida que las legales y pueden ganar en eficacia.

En la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas de la Comisión:

- Se introduce el concepto de *comunicaciones de mercadotecnia directa* y se unifica el tratamiento de los distintos medios de comunicación (sistemas automatizados de llamada, comunicación con interacción humana o sin ella, correo electrónico, SMS, etc.). Se da solución conjunta al tratamiento de todas las comunicaciones, que se realizan a través de diferentes medios de comunicación.
- Se refiere a las personas físicas y jurídicas.
- Se determina que aun en el caso de haber obtenido el consentimiento, deben establecerse claramente mecanismos o procedimientos de oposición al envío de comunicaciones comerciales.
- Se mantiene la excepción del actual artículo 21.2 LSSICE, para el envío de comunicaciones comerciales sin el consentimiento previo.
- Se mantienen los deberes de información en relación al carácter comercial de estas comunicaciones comerciales.

Lectura recomendada

Sobre estas cuestiones, véase:

«Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)». Disponible en: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103.

4.5. El marketing viral

Otro supuesto que hay que tener en cuenta es el marketing viral. Lo que hacen las comunicaciones comerciales de naturaleza viral es un reenvío a terceros por parte del destinatario de una comunicación electrónica comercial. Según el estudio de Telefónica titulado «Nuevas forma de marketing: el marketing viral» (disponible en: http://www.agpd.es/portalwebAGPD/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/pg_nuevas_formas_marketing_vi_encuentro.pdf), se trata de «técnicas de marketing que utilizan el efecto "red social" creado por Internet y los móviles». Se afirma también que son «planes fáciles de ejecutar: atraer con productos atractivos e incluso gratuitos, a través de un medio de difusión sencillo (e-mail, sitio web, descarga de software, SMS); utilizan el contacto de redes humanas de comunicación y obtienen ventajas de los recursos de los demás».

Siguiendo a Álvarez Hernando, no tendrían la consideración de comunicación comercial, según la LSSICE, los reenvíos a terceros por el receptor siempre que la comunicación sea elaborada por un tercero (por ejemplo, podría ser el anunciante) y cuando no exista compensación económica, es decir, cuando no se incentive la remisión del correo mediante una ventaja o recompensa.

Referencia bibliográfica

J. Álvarez Hernando (2014). «Publicidad, comunicaciones comerciales y protección de datos». En: *Practicum de Protección de Datos 2015*. Cizur Menor: Aranzadi.

5. Publicidad y prospección comercial

5.1. La publicidad en Internet

Internet ha multiplicado y variado las formas de hacer publicidad, propiciando la aparición de nuevas fórmulas y consiguiendo una publicidad cada vez más personalizada. Estas nuevas fórmulas implican en muchas ocasiones un seguimiento detallado de hábitos y gustos del consumidor, lo que conlleva, en prácticamente todos los casos, el uso de datos personales de cada usuario, a veces a través de *cookies* y otras mediante diferentes herramientas tecnológicas. En este marco tenemos, entre otras, la publicidad contextual, la publicidad segmentada, la publicidad comportamental *online* o la publicidad social *online* (o *social advertising*).

Lecturas recomendadas

Sobre estas cuestiones, véase:

S. Navas Navarro (2016). «*Cookies* y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal». En: Navas Navarro, S.; Camacho Clavijo, S. *Mercado Digital. Principios y reglas jurídicas*. Valencia: Tirant lo Blanch (págs. 357-380).

Grupo de Trabajo del Artículo 29 (2010). «Dictamen 2/2010 sobre publicidad comportamental en línea». Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf.

Por su parte, el Código Ético de Confianza Online se refiere a la captación de datos con fines publicitarios en grupos de noticias, foros, chats o similares. En este sentido, afirma que: «No podrán utilizarse los grupos de noticias, tablones de anuncios, foros o las charlas para captar datos con finalidad publicitaria, salvo que dicha recogida se ajuste a las normas de obtención de datos establecidas en el presente Código».

Por lo que se refiere a la publicidad, y también con carácter general al diseño de páginas web, resulta muy interesante en lo relativo a la protección de datos de carácter personal el artículo 25 del Reglamento General de Protección de Datos, que lleva por título «La protección de datos desde el diseño y por defecto». Se unen así los aspectos jurídicos y los tecnológicos para garantizar la protección de datos de los usuarios desde el mismo momento de la creación de nuevas aplicaciones.

El considerando 78 del RGPD ya se refiere a la protección de datos desde el diseño y por defecto. Estas medidas pueden consistir en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y al tratamiento de datos, permitiendo a los interesados supervisar el tratamiento y al responsable crear y mejorar elementos de seguridad. Y añade que hay que alentar a los creadores de productos, servicios y aplicaciones que tengan en cuenta el derecho a la protección de datos cuando diseñen y desarrollen sus productos.

La protección de datos desde el diseño se vincula al estado de la técnica, al coste de la aplicación y a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como a los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas. El responsable del tratamiento aplicará medidas técnicas y organizativas apro-

piadas, como la seudonimización, la minimización de datos, así como la integración de las garantías necesarias en el tratamiento, a fin de cumplir lo dispuesto en el RGPD y proteger los derechos de los interesados.

El artículo 25 RGPD también se refiere a la protección de datos por defecto. En este caso, determina que se aplicarán las medidas técnicas y organizativas necesarias para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada uno de los fines específicos del tratamiento. Esta medida garantizará que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Con estas medidas se implica de igual modo a las empresas para que, desde un punto de vista tecnológico y desde el propio diseño de sus aplicaciones, garanticen al máximo la protección de los datos personales de los usuarios de sus aplicaciones.

Estos conceptos, que ya eran conocidos a nivel internacional, se introducen ahora en el RGPD, que aborda la protección de datos de carácter personal de forma preventiva, es decir, *ex ante*.

Lectura recomendada

Sobre esta cuestión, véase:

R. Duaso Calés (2016). «Los principios de protección de datos desde el diseño y protección de datos por defecto». En: Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (págs. 295-333).

Por lo que se refiere a los sujetos intervinientes, el artículo 8 de la Ley General de Publicidad, define los términos **anunciante** y **agencias de publicidad**. Según dicho artículo, es anunciante «la persona natural o jurídica en cuyo interés se realiza la publicidad» y son agencias de publicidad «las personas naturales o jurídicas que se dediquen profesionalmente y de manera organizada a crear, preparar, programar o ejecutar publicidad por cuenta del anunciante». También define **medios de publicidad** como «las personas naturales o jurídicas, públicas o privadas que, de manera habitual y organizada, se dediquen a la difusión de publicidad a través de los soportes o medios de comunicación social cuya titularidad ostenten».

En relación a las partes intervinientes, la «Guía para el uso de *cookies*» de la Agencia Española de Protección de Datos (disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf) se refiere a los distintos intervinientes. Lo hace en estos términos:

«**B. Partes intervinientes**

i. Usuario

Es el destinatario, persona física, que accede al servicio prestado por un editor, pudiendo diferenciarse entre usuario registrado y no registrado. No obstante utilizarse, en la normativa legal, el término destinatario del servicio, en la presente guía se emplea el término usuario, por ser este de uso más común.

ii. Editor

Es cualquier entidad prestadora de servicios de la sociedad de la información titular de una página web a los que puede acceder un usuario y para cuya prestación se utilizan *cookies*.

Por ejemplo, este sería el caso del titular de una carpintería o de una pescadería que disponga de una página web a través de la cual ofrezca simplemente información relacionada con los servicios que presta o disponga de una tienda on-line a través de la cual se puedan efectuar transacciones comerciales o haya creado una aplicación para móviles para cuyo funcionamiento puede ser necesario la utilización de *cookies*.

Algunos editores, además de prestar un servicio a los usuarios, ofertan actuando como soportes por si mismos o con la ayuda de uno o varios terceros, espacios publicitarios a los anunciantes para cuya gestión es necesaria la utilización de *cookies*.

Este sería, por ejemplo, el caso de una revista o de un medio de comunicación que presta a los usuarios un servicio de información a través de una página o una aplicación móvil y, a su vez, ofrece junto a esta información publicidad sobre los servicios, los productos o la imagen de uno o varios anunciantes.

A la luz de esta definición, se puede observar el doble papel o función que puede desarrollar un editor. Actúa como prestador de un servicio al usuario, para cuya prestación puede ser necesaria la utilización de *cookies*. Cuando actúa como soporte, puede además ofertar a los anunciantes espacios publicitarios que estarán gestionados bien por el mismo editor o bien por una o más entidades simultáneamente, mediante el uso de tecnologías que pueden requerir el uso de *cookies* para su funcionamiento.

iii. Anunciante

Es la entidad cuyos productos, servicios o imagen se publicitan a través de los espacios publicitarios de los que disponen, en su caso, los editores en sus páginas u otras aplicaciones desde las que prestan los servicios a los usuarios. En este sentido, actúa como demandante de espacios publicitarios.

Frecuentemente, el editor también suele actuar como anunciante. En estos casos, el editor actúa como anunciante desde el momento en que, para realizar publicidad del servicio que presta a los usuarios, se sirve de los espacios publicitarios que ponen a su disposición otros editores.

Este sería el caso, por ejemplo, en el que el titular de una carpintería o de una pescadería, cuando además de actuar como editor de su propia página web desde la que presta el servicio, actúa como anunciante al contratar la difusión publicitaria de sus productos o servicios directamente con otro editor, editores o, indirectamente, con una red publicitaria.

iv. Agencias de publicidad y agencias de medios

Son entidades que se encargan del diseño y la ejecución de publicidad, así como de la creación, preparación o programación de las campañas publicitarias de los anunciantes, actuando en nombre y por cuenta de estos en la contratación de espacios publicitarios. En este sentido, también se les puede considerar como demandantes de espacios publicitarios para los anunciantes.

v. Redes publicitarias

Son un conjunto de entidades que, actuando en nombre y representación directa o indirectamente de uno o varios editores, ofrecen, también directamente a los anunciantes o, indirectamente a través de otros demandantes, como las Agencias de publicidad, la posibilidad de obtener espacios publicitarios o algún tipo de resultado concreto como *clicks*, ventas o registros, a través de la gestión y el tratamiento de los datos obtenidos de la utilización de las *cookies* descargadas o almacenadas en los equipos terminales de los usuarios, cuando estos acceden a los servicios prestados por el editor.

La finalidad de la labor de estas entidades es llevar a cabo, de la mejor manera posible, la gestión del inventario de espacios publicitarios, cuya titularidad corresponde a los editores, de forma que converja con la demanda de los anunciantes.

Es el editor quien decide si la totalidad o parte del inventario del que dispone es gestionado por una entidad en exclusiva o por varias entidades simultáneamente, en función de los criterios que establezca.

Este tipo de entidades suelen realizar una agregación de la oferta de los espacios publicitarios y de los inventarios de varios editores.

Algunas de estas entidades, mediante las *cookies* que gestionan, recaban información de los hábitos de navegación de los usuarios que acceden a los servicios o páginas ofrecidos por cualquiera de los editores a quienes representan. Los datos se recogen con la finalidad de que la difusión de las piezas publicitarias de los anunciantes sea lo más eficiente posible. Para ello analizan los hábitos de los usuarios en Internet con el fin de ofrecerles la publicidad más adecuada a los intereses asociados a su perfil de navegación. Este tipo de entidades actúan en el lado de la oferta como ofertantes de espacios en nombre y representación, directa o indirectamente, de uno o varios editores.

A pesar de que este tipo de entidades muestran a sus clientes de manera agregada los datos obtenidos como resultado de la utilización de las *cookies*, será necesario informar y obtener el consentimiento de los usuarios para la recogida de dichos datos y su agregación y tratamiento posterior con la finalidad de gestionar la oferta de los espacios de los editores. Generalmente, se realizará desde la página web de los editores que usen este tipo de *cookies* propias o de terceros.

Para llevar a cabo la gestión de estos espacios publicitarios de la forma más eficaz posible, se emplean diferentes tipos de equipos, tecnologías, programas o aplicaciones de gestión, como adServers, adExchanges, etc., que tratan en tiempo real los datos obtenidos, de forma que las piezas publicitarias de los anunciantes se incluyen en los espacios publicitarios de los editores de manera automática, en función de los criterios que se establezcan en cada caso.

Finalmente, también es necesario señalar que es frecuente que esta labor de gestión sea subcontratada de forma total o parcial a otras empresas especializadas en el desarrollo de las actuaciones necesarias para la gestión de los espacios publicitarios.

vi. Empresas de análisis y medición

Son entidades que miden y/o analizan el comportamiento de la navegación de los usuarios en la página web de un editor, actuando en su nombre y representación, a través del análisis de los datos obtenidos mediante la utilización de las *cookies*, con la finalidad de mejorar el servicio que presta el editor.

Por regla general, para la prestación de este tipo de servicios se utilizan lo que se denominan "*cookies* de terceros", es decir, *cookies* que son enviadas al equipo terminal del usuario no desde un equipo o dominio gestionado y controlado por el editor, sino desde un equipo o dominio gestionado por la propia entidad que realiza el análisis de los datos.

Dada la multiplicidad de entidades intervinientes, corresponderá a cada una analizar la labor que desarrolla para posicionarse en uno u otro papel de cara a la determinación de la responsabilidad en la que incurren y al cumplimiento de las obligaciones establecidas en la normativa y desarrolladas en la presente guía.»

De acuerdo con la normativa, es importante la identificación de todos los mensajes publicitarios como tales, lo que también establece la nueva Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas. Según su artículo 16, las personas que utilicen servicios de comunicaciones electrónicas para efectuar llamadas de mercadotecnia directa deberán presentar la identificación de una línea en la que se les pueda contactar o presentar un código o prefijo específico que permita identificar que se trata de una llamada de mercadotecnia. Y añade en el apartado cuarto del mismo artículo que quien utilice servicios de comunicaciones electrónicas para transmitir comunicaciones de mercadotecnia directa deberá informar a los usuarios finales del carácter comercial de la comunicación y de la identidad de la persona física o jurídica en nombre de la cual se transmite. Por otra parte, también se debe proporcionar la información necesaria a los destinatarios para que puedan ejercer fácilmente su derecho a retirar su consentimiento para no recibir nuevas comunicaciones de mercadotecnia.

Otras formas de publicidad en Internet que enumera y describe la «Guía para el uso de *cookies*» de la Agencia Española de Protección de Datos (disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf) son:

«*Espacio publicitario*: es un lugar en el que el editor prevé, cuando programa la página web, que aparezca la publicidad de los productos, la imagen o los servicios de los anunciantes. Existe una gran variedad de espacios o formatos publicitarios; desde los que se integran en la propia aplicación como los *banners*, rascacielos, robapáginas, botones y los enlaces de texto, hasta los denominados flotantes como los *pop ups*, *layers*, cortinillas o *interstitials* de tránsito, etc.

Banner: anuncio con forma de rectángulo horizontal ubicado en la parte superior de las páginas web y que puede usar tecnología gif, animado, flash o jpeg.

Rascacielos: anuncio con forma de rectángulo vertical ubicado en los laterales de las páginas web y que puede usar tecnología gif, flash o jpeg.

Robapáginas: anuncio con forma cuadrada generalmente integrado en una ubicación fija de una página

Pop up: formato que aparece como una ventana emergente sobre una ventana del navegador abierta.

Layers: formato flotante que se superpone al contenido de la página y que se mueve por la pantalla

Cortinillas o *interstitials* de tránsito: anuncios que aparecen entre dos páginas dentro de una web. También conocidos como "páginas de bienvenida" y "anuncios de transición".»

En relación con la publicidad y las redes sociales, es interesante el «Dictamen 5/2009 sobre las redes sociales en línea» del Grupo de Trabajo del Artículo 29 (disponoble en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf). Según este documento:

«La comercialización directa constituye una parte esencial del modelo comercial de los SRS, que pueden utilizar diferentes modelos de comercialización. No obstante, la comercialización que utilice los datos personales de los usuarios debería cumplir las disposiciones aplicables de la Directiva relativas a la protección de datos y sobre la vida privada y las comunicaciones electrónicas.

La *comercialización contextual* se adapta al contenido visto por el usuario o al que accede este.

La *comercialización segmentada* consiste en difundir publicidad a grupos de usuarios específicos; se coloca al usuario en un grupo en función de la información que ha comunicado directamente al SRS.

Por último, la *comercialización de comportamiento* selecciona la publicidad basándose en la observación y el análisis de la actividad del usuario a lo largo del tiempo. Estas técnicas pueden estar sujetas a requisitos jurídicos, dependiendo de las bases jurídicas aplicables y de las características de las técnicas utilizadas. El Grupo de Trabajo recomienda no utilizar datos sensibles en los modelos publicitarios de comportamiento, a menos que se cumplan todos los requisitos jurídicos.

Cualquiera que sea el modelo o la combinación de modelos utilizados, la publicidad puede ser difundida directamente por el SRS (el proveedor de SRS ejerce aquí una actividad de intermediario), o por un publicitario tercero. En el primer caso, los datos personales de los usuarios no deben revelarse a terceros. Sin embargo, en el segundo caso, el publicitario tercero probablemente tratará los datos personales de los usuarios, en particular, si trata la dirección IP del usuario o una *cookie* situada en el ordenador de este.»

Existen también prácticas publicitarias que no se consideran lícitas, entre otras: la publicidad encubierta en páginas web, o publicidad y mensajes publicitarios no identificados como tales, y la introducción de enlaces inadecuados o ilícitos o de enlaces que lleven a engaño, como un *link* a un servicio gratuito que después conecta con un 906.

Lectura recomendada

Sobre estas prácticas, véase:

Grupo Telefónica (2008). «Nuevas forma de marketing: el marketing viral». Disponible en http://www.agpd.es/portalwebAGPD/internacional/red_iberoamericana/encuentros/VI_Encuentro/common/pg_nuevas_formas_marketing_vi_encuentro.pdf

En referencia a las conocidas como *pop ups* o ventanas emergentes, hubo una demanda en EE.UU. contra la empresa «Celebrity Cruises», en el estado de Utah. Se enviaba una ventana emergente que incitaba a los lectores a participar en un concurso para ganar un crucero gratis. El anuncio aparecía en pantalla (en mayo de 2003) cuando se visitaba la página del periódico *Los Angeles Times*. En ese momento, se estableció que no se trataba de *spam*, ya que no se enviaban mensajes a una dirección de correo. Parece que tendrían que ser las medidas tecnológicas las que lograran evitar estas prácticas.

Se entendía que solo eran ilícitos cuando estuvieran fuera de los límites (publicidad engañosa, prácticas desleales o si contienen *spyware* u otros). No puede considerarse lícita la práctica publicitaria de presentar series de anuncios que solo se pueden parar apagando el ordenador.

La «Guía para la lucha contra el spam» (disponible en: https://portal.uah.es/portal/page/portal/proteccion_datos/repositorio/guiacontraelspam.pdf) se refiere al «spam por ventanas emergentes (*pop ups*)». Lo hace en estos términos:

> «Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a Internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows titulado "servicio de visualización de los mensajes". Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario. Para ello se utiliza una funcionalidad del sistema de explotación Windows, disponible sobre las versiones Windows NT4, 2000, y XP, y que permite a un administrador de redes enviar mensajes a otros puestos de la red. La solución más sencilla para evitar estas ventanas emergentes consiste en desactivar este servicio de Windows. Otro método consiste en utilizar un cortafuegos destinado a filtrar los puertos TCP y UDP (135, 137,138, 139 y 445) de su ordenador, pero con esta medida es posible que deje de funcionar la red.»

El Código Ético de Confianza Online, al referirse a la publicidad en Internet, establece que esta no podrá impedir la libre navegación del usuario. En su artículo 12.2, añade además que: «En particular, los mensajes publicitarios que reciba el usuario durante su navegación por una página web deberán permitirle en todo momento salir del mensaje publicitario o eliminarlo de su pantalla, y volver a la página de origen desde la que el usuario accedió al mensaje publicitario». Mientras que el artículo 32 se refiere a otra práctica publicitaria, la captación de datos personales en grupos de noticias, foros, charlas (chats) y similares con finalidad publicitaria: «No podrán utilizarse los grupos de noticias, el tablón de anuncios, los foros o las charlas para captar datos con finalidad publicitaria, salvo que dicha recogida se ajuste a las normas de obtención de datos establecidas en el presente Código».

Por lo que se refiere a la instalación de *spyware* u otros programas para obtener información del usuario, no sería lícita la instalación de software si no se informa de su contenido a los consumidores. No pueden olvidarse todos los deberes de información en los contratos celebrados con consumidores que establece tanto la Directiva comunitaria sobre protección de los consumidores (Directiva 2011/83/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo; disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32011L0083&from=ES), como el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (TRLGDCU) y otras normas específicas para contratos concretos.

Es muy importante, en definitiva, que las novedades tecnológicas sean compatibles con la privacidad y la protección de datos, algo que parece dejar bien asentado el Reglamento General de Protección de Datos en su ya comentado artículo 25, dedicado a la privacidad desde el diseño.

5.2. El tratamiento de datos en campañas publicitarias: entidades implicadas y responsabilidades. Los artículos 30 y 31 LOPDP y los artículos 45 a 51 del RDLOPDP

El tema relativo al tratamiento de datos para fines publicitarios y de prospección comercial deja patente –incluso con más claridad que en otras ocasiones– la existencia de intereses encontrados entre las empresas de marketing directo y el consumidor. Las cuestiones que se plantean y que nos pueden ayudar a ir analizando el tema, desde el punto de vista de la salvaguarda de la privacidad del destinatario, son muchas y variadas. Entre ellas:

- ¿Cuándo se pueden utilizar datos personales para enviar publicidad lícitamente?
- ¿Qué datos pueden utilizarse?
- ¿Quién responde de ese envío?
- ¿Cuáles son las consecuencias de un envío en contra de lo que establecen las normas?
- ¿Y las consecuencias del envío de publicidad a las listas de exclusión?
- ¿Qué supone en todo ello la aprobación del RGPD?

Referencia bibliográfica

Este apartado se fundamenta en:

A. Paniza Fullana (2009). «Tratamientos para actividades de publicidad y prospección comercial». En: Varios autores. *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPDP*. Valencia: Tirant lo Blanch (págs. 237-255).

Además, no se puede olvidar que el RGPD convive en el ordenamiento jurídico con otras normas, por lo que habrá que analizar en qué medida les puede afectar, qué relación existe entre ellas, entre otros aspectos.

5.2.1. En general

La regulación a día de hoy se encuentra en los artículos 45 a 51 RDLOPDP y trae causa de los artículos 30 y 31 LOPDP.

El artículo 30 LOPDP se refiere a los tratamientos con fines de publicidad y de prospección comercial: quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas podrán utilizar nombres y direcciones u otros datos de carácter personal lícitamente en dos situaciones:

- Cuando estos figuren en fuentes accesibles al público o se hayan obtenido de los propios interesados.
- Cuando se haya obtenido el consentimiento del interesado.

Por su parte, el artículo 31 LOPDP es el que se dedica al censo promocional y lo hace en estos términos:

> «1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.
>
> 2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.
>
> 3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.
>
> 4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.»

Este censo, que parece no haber tenido demasiada trascendencia práctica, incluye el nombre, los apellidos y el domicilio que aparecen en el censo electoral y se solicita al Instituto Nacional de Estadística u otros órganos equivalentes de la Comunidad Autónoma. El uso de esta lista tendrá un plazo de vigencia de un año, transcurrido el cual perdería el carácter de fuente accesible al público.

También establece este artículo que los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente y deberán ser gratuitos, actualizarse trimestralmente y se podrá exigir una contraprestación para facilitar la lista en soporte informático.

¿Cómo se desarrollan estos preceptos en el RDLOPDP? El tema del tratamiento para fines de publicidad y prospección comercial se trata, como decíamos, en los artículos 45 a 51. Estos artículos van desde el consentimiento necesario para el tratamiento para fines de publicidad y prospección comercial hasta los derechos de acceso, rectificación, cancelación y oposición, además del tratamiento de datos en campañas publicitarias y los ficheros de exclusión.

El primero de los preceptos dedicados a este tema en el RDLOPDP, el artículo 45, se refiere así a los datos susceptibles de tratamiento e información al interesado:

> «1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, solo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:
>
> a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.
>
> b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.
>
> 2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.
>
> A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.»

Desde el punto de vista subjetivo, es más amplio que el artículo 30 de la LOPDP ya que se refiere, igual que aquel artículo, a quienes de dediquen a la recopilación de direcciones, al reparto de documentos, a la publicidad, la venta a distancia, la prospección comercial y otras actividades análogas; pero añade, además, a quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros. Es decir, abarca tanto a quien publicite sus propios productos como a quien lo haga a través de una empresa especializada en estas actividades.

Estas personas solo podrán utilizar «nombres, direcciones u otros datos de carácter personal» cuando figuren en alguna de las fuentes accesibles al público (artículo 3.j) LOPDP y artículo 7 del RPD), siempre que el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento y, precisamente, para las actividades previstas en este artículo, es decir, que no se haya opuesto a su tratamiento para fines publicitarios o que hayan sido facilitados por los propios interesados u obtenidos con su consentimien-

to, pero ese consentimiento debe haber sido recabado para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial.

Queda patente el carácter estricto de estos artículos en lo que se refiere al consentimiento del afectado, incluso en el caso de datos que proceden de fuentes accesibles al público y se destinan a publicidad o prospección comercial. En este caso, hay que informar al interesado en cada comunicación sobre el origen de los datos y la identidad del responsable del tratamiento, los derechos que le asisten y ante quién podrá ejercitarlos.

Además, hay que informar de que sus datos provienen de una fuente accesible al público y de la entidad de la que hubieran sido obtenidos. Es un artículo bastante exigente tanto en el ámbito subjetivo como en los requisitos a cumplir para el tratamiento de datos con fines publicitarios.

La resolución 457/2006 de la AEPD se refería a la siguiente cláusula:

«Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de XXX para gestionar la relación comercial con usted [...]. Es posible que en un futuro –incluso finalizada nuestra relación comercial– utilicemos sus datos personales para informarle sobre nuestros productos y/o servicios o que comuniquemos tales datos a las empresas que integran el grupo mercantil YYY, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollan su actividad en los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, con el fin de que le informen sobre los productos o servicios que comercialicen.»

La resolución afirma que, en relación con el artículo 5.1.a) LOPDP, la citada cláusula no concreta de modo expreso, preciso e inequívoco la finalidad de la recogida de los datos y de los destinatarios de la información «ya que se refiere a términos inconcretos de los que no cabe deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos, lo que impide que el interesado pueda conocer como señala el T.C. a qué uso lo está destinando y, por otro lado, el poder oponerse a esa posesión y usos».

En otro caso resuelto por la resolución 682/2005 de la AEPD, «el tratamiento de datos efectuado queda al margen de los supuestos permitidos en el artículo 6 LOPDP, pues ni los datos fueron obtenidos de fuentes accesibles al público ni el tratamiento se efectuó con consentimiento del denunciante». Y la resolución 647/2005 considera válido el mecanismo consistente en recoger la cláusula informativa en el documento por el que el propio afectado facilita los datos y consiente el tratamiento con las finalidades específicas que se indiquen. Obviamente, así deben considerarse siempre que se disponga del documento en el que conste la manifestación de voluntad del titular de los datos.

Consentimiento e información al interesado son dos puntos clave en todo el tema del tratamiento de datos para fines publicitarios y prospección comercial.

En la resolución 580/2005 de la AEPD se resuelve un caso en el que Don P.M.F. había recibido un envío publicitario en el que constaba como responsable del fichero la empresa XXX. Se cita al destinatario a acudir a un hotel para recoger un regalo. Se pregunta por el origen de los datos y se afirma que proceden de Páginas Blancas On Line de Telefónica, lo que no se acredita. Afirma la resolución que: «Este tratamiento tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una ley que ampara el tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato». En este caso no quedó acreditado que ninguna de las empresas implicadas contara con el consentimiento del denunciante para el tratamiento automatizado de sus datos de carácter personal, ni tampoco que dichos datos hubieran sido obtenidos de alguna fuente accesible al público. Por ello, ha de entenderse conculcado el principio de consentimiento del artículo 6 LOPDP. En sentido parecido se expresa la resolución de la AEPD 150/2006.

5.2.2. Las fuentes accesibles al público

No se puede obviar en ningún momento que el tema del consentimiento del interesado subyace en todos y cada uno de los supuestos:

- En sentido positivo: datos que «hayan sido facilitados por los propios interesados u obtenidos con su consentimiento».

- En sentido negativo: que provengan de fuentes accesibles al público y «el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento».

Es a este segundo supuesto al que dedicaremos este apartado. Según el artículo 45 RDLOPDP, se podrán utilizar nombres y direcciones y otros datos de carácter personal en el caso que provengan de alguna de las fuentes accesibles al público a las que se refieren los artículos 3 j) LOPDP y el artículo 7 RDLOPDP. Pero, ¿qué son las **fuentes accesibles al público**?

En primer lugar, se trata de resolver el encaje del artículo 45 RDLOPDP, el artículo 3 LOPDP y el artículo 7 también del RDLOPDP. La principal cuestión a destacar es que este artículo 7 RDLOPDP parece ampliar el listado de fuentes accesibles al público del artículo 3 j) LOPDP. Analicemos ambos preceptos.

Según el artículo 3 j) LOPDP, 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». Y lo son:

- El censo promocional (artículo 31 LOPDP ya citado: datos de nombre, apellidos y domicilio que constan en el censo electoral). Censo que, por otra parte, no está operativo en la práctica.

- Los repertorios telefónicos en los términos de su normativa específica.

- 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.

- Los diarios y boletines oficiales.

- Los medios de comunicación.

Repertorios telefónicos

En cuanto a las guías telefónicas, los datos de puerta y número del domicilio de los afectados no se publican en las guías de abonados de los servicios telefónicos, por lo que no pueden considerarse datos que provengan de fuentes accesibles al público. Así lo ha constatado en numerosas ocasiones la Agencia de Protección de Datos. El artículo 30.4 del Reglamento sobre las Condiciones para la Prestación de Servicios de Comunicaciones Electrónicas, el Servicio Universal y la Protección de los Usuarios aprobado por Real Decreto 424/2005, de 15 de abril, afirma que: «En relación a los datos de cada abonado deberá figurar, al menos, la siguiente información: a) nombre y apellidos, o razón social; b) número o números de abonado; c) dirección postal del domicilio, excepto piso, letra y escalera; d) terminal específico que deseen declarar en su caso; e) nombre del operador que facilite el acceso a la red».

Además, el artículo 28.3 LOPDP establece que las fuentes accesibles al público que se editen en forma de libro o algún otro soporte físico perderán el carácter de fuente accesible al público con la nueva edición que se publique y si se obtiene telemáticamente una copia de la lista en formato electrónico perderá el carácter de fuente accesible al público en el plazo de un año, contado desde el momento de su obtención. También queda patente en las resoluciones de la AEPD que los buzones de correo no son fuentes accesibles al público.

Colegios Profesionales

En la resolución 562/2005 se procede a analizar la alegación de un colegio profesional, concretamente el COPAC, en el sentido de que los datos de los colegiados proceden de una fuente accesible al público: «En el presente caso no ha quedado acreditado que el COPAC edite un fichero de sus colegiados que pueda ser consultado por cualquier persona, es decir, no edita ni ha editado nunca anuario alguno conteniendo datos relativos a los profesionales colegiados. El propio denunciante ha comunicado que, de forma reiterada, ha solicitado dicho fichero para comunicarse con el resto de los colegiados y el COPAC le ha denegado el acceso al mismo. Por lo tanto, en el presente caso, la lista de colegiados de COPAC no tiene el carácter de fuente accesible al público».

Por su parte, el artículo 7 RDLOPDP añade «Las guías de servicios de comunicaciones electrónicas en los términos previstos en su normativa específica». Sin embargo, esta cuestión no es tan sencilla. Parece que la remisión a la «normativa específica» se refiere al artículo 38.6 y a la disposición adicional 9ª de la Ley General de Telecomunicaciones, que permite a los prestadores de servicios de comunicaciones electrónicas y de servicios de información elaborar y comercializar guías de abonados comunicándolas a terceros sin necesidad de obtener el consentimiento de los abonados, eso sí, dejando a salvo el derecho del abonado a la protección de sus datos de carácter personal, incluido el de no figurar en dichas guías. Parece, sin embargo, que este artículo está pensando en guías telefónicas, no de correo electrónico, ya que si fuera así iría en contra de la LSSICE que prevé el sistema *opt in* para el envío de comunicaciones electrónicas, es decir, solo se pueden enviar comunicaciones comerciales con el consentimiento previo del interesado, ni siquiera se podrán enviar si los datos

provienen de una fuente accesible al público. La LSSICE solo excluye la necesidad de consentimiento en el caso de su artículo 21.2, que hace referencia a la existencia de una relación contractual previa.

La Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas define **guía accesible al público** como «una guía de usuarios finales de servicios de comunicaciones electrónicas en formato impreso o electrónico que se publica o se pone a disposición del público o de una parte del público, entre otros medios a través de un servicio de información». La regulación de las guías accesibles al público está en el artículo 15, distinguiendo entre personas físicas y jurídicas. Según este precepto:

- Es necesario el consentimiento previo de los usuarios finales personas físicas para incluir sus datos personales en la guía, así como para incluir los datos por categorías en tanto sean pertinentes para la finalidad de la guía, según lo determinado por el proveedor de la lista.

- Los proveedores deberán facilitar los medios para comprobar, corregir o suprimir esos datos.

- Los proveedores de guías deberán informar a los usuarios finales de las funciones de búsqueda de que dispone la guía y obtener su consentimiento antes de habilitar esas funciones en relación con sus datos.

- Los proveedores de guías ofrecerán a los usuarios finales personas jurídicas la posibilidad de oponerse a la introducción de sus datos en la guía y les facilitarán los medios para comprobar, corregir o suprimir esos datos.

- Se ofrecerá gratuitamente a los usuarios finales la posibilidad de no figurar en una guía accesible al público, así como de comprobar, corregir o suprimir los datos que les conciernen.

En el caso de las listas de personas pertenecientes a grupos de profesionales, el artículo 7 RDLOPD establece que la dirección profesional podrá incluir la dirección electrónica.

Estamos de nuevo ante el problema planteado anteriormente: la LSSICE que exige el consentimiento previo para el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, dejando a salvo la excepción del artículo 21.2.

El Reglamento también cierra este listado con los diarios oficiales y medios de comunicación social. Y en todos ellos, igual que en la LOPDP, para que puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación.

Se pueden comparar ambos artículos:

Artículo 3 j) LOPDP	Artículo 7 RDLOPDP
Censo promocional	Censo promocional, regulado conforme a la LOPDP
Los repertorios telefónicos en los términos previstos en su normativa específica	Las guías de servicios de comunicaciones electrónicas, en los términos previstos en su normativa específica
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.	Igual, pero añade: «La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. 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.»
Los diarios y boletines oficiales	Los diarios y boletines oficiales
Los medios de comunicación	Los medios de comunicación

La Sentencia de la Audiencia Nacional de 11 de diciembre de 2011 afirma que los datos obtenidos de Internet no se consideran obtenidos de una fuente accesible al público. En este caso, la parte recurrente pretende que se considere que los datos de las direcciones IP proceden de una fuente accesible al público, por lo que su tratamiento no exigiría el consentimiento como excepción a la regla general que señala el artículo 6.1 LOPDP. Afirma el tribunal que no puede admitirse este razonamiento por falta de su elemento básico. Se refiere a las definiciones del artículo 3 j LOPDP y al RDLOPDP y concluye afirmando que:

«Por lo tanto, y sin que sean necesarias mayores consideraciones sobre la cuestión, las direcciones IP que pudiera conseguir la entidad ahora recurrente mediante el uso de un determinado programa informático son datos de los que en ningún caso puede entenderse que procedan de fuentes accesibles al público por el simple hecho de que aparezcan en Internet y no puede aplicarse la excepción a la exigencia de consentimiento al tratamiento que deriva del artículo 6.2 de la LOPD.

Esta Sala se ha pronunciado en diversas ocasiones sobre que la información que aparece en Internet no es una información que se pueda entender procedente de fuentes accesibles al público; así resulta, entre otras, de las sentencias dictadas en los recursos 163/2006 (RJCA 2007, 675), 220/2007 o 589/2008 (JUR 2010, 17665).

Obviamente, tampoco puede aplicarse el artículo 6.1 de la LOPD que exige para el tratamiento de datos el consentimiento del interesado sobre la base de considerar que existe un consentimiento tácito por resultar visibles las direcciones IP cuando se interviene en programas P2P. El consentimiento que previene el artículo 6.1 de la LOPD podrá ser tácito pero, en cualquier caso, deberá ser inequívoco y dicha condición no resulta por la transparencia de las direcciones IP en Internet.

En cualquier caso, y aunque se entendiera que pudiera existir consentimiento tácito, resulta que nunca podrá entenderse prestado para un tratamiento tan específico y determinado como el que se pretende: aplicar un programa informático para determinar las direcciones IP de quien utiliza en determinada medida los programas de descarga fonográfica y musical.»

Respecto a la segunda cuestión planteada, es decir, los requisitos que tiene que cumplir el encargado del tratamiento, aun en los casos en los que los datos provengan de fuentes accesibles al público, hay que decir que, aunque los

datos procedan de fuentes accesibles al público, el responsable no está exento del cumplimiento de una serie de requisitos que se encarga de establecer el artículo 45.2 RDLOPD:

> «[...] deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.
>
> A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.»

Resulta especialmente interesante la cuestión de sobre quién recae la carga de la prueba del contenido de los datos en fuentes accesibles al público. A este tema hace referencia la resolución de la AEPD 248/2005:

> «[...] debe tenerse en cuenta que a la Administración le resultaba imposible comprobar todos y cada uno de los ficheros accesibles por el público existentes en España o en el extranjero. En cambio a la recurrente, si en verdad no obtuvo los datos del censo, le resultaba muy sencillo citar la fuente de origen de los datos. Pues bien, tampoco lo ha hecho. Se ha limitado en el período probatorio a pedir información en relación con la inclusión del denunciante en todos los listines telefónicos y, nada menos, que en relación con todos los colegios provinciales de unas diez titulaciones profesionales. Si en verdad no tomó los datos del censo para desvirtuar la prueba en que se basa la Administración, ha debido manifestar de dónde tomó los datos y no dar "palos de ciego" como ha hecho.»

Y según la Sentencia de la Audiencia Nacional de 11 de mayo de 2001:

> «[...] quien gestiona la base debe estar en condiciones de acreditar el consentimiento del afectado [...] siendo carga de la prueba del mismo su justificación y la entidad recurrente en ningún momento ha realizado esfuerzo probatorio tendente a la acreditación del consentimiento de las personas en las que se basa la sanción.»

Lecturas recomendadas

Sobre esta cuestión, véase:

M. Vilasau Solana (2008). «¿Cómo llegar al consumidor? Entre la protección de datos y la legislación sobre la sociedad de la información». *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 3, págs. 83-101).

M. Vilasau Solana (2011). «Consentimiento, fuentes accesibles al público e interés legítimo como mecanismos que legitiman el tratamiento de datos de carácter personal». En: Blasco Gascó, F. y otros (coords.). *Estudios jurídicos en homenaje a Vicente L. Montés Penadés*, tomo II. Valencia: Tirant lo Blanch (págs. 2877-2898).

5.2.3. Consentimiento y finalidades

Según el artículo 45.1.b) del RDLOPDP, se podrán utilizar datos de carácter personal cuando estos hayan sido facilitados por los propios interesados u obtenidos con su consentimiento «para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o de prospección comercial».

De ello se extrae que el afectado tiene que saber para qué se van a utilizar sus datos personales. Una definición o descripción general no satisface el principio de la finalidad y los datos utilizados para una determinada finalidad no podrán ser utilizados para otra incompatible. Todo ello no es más que la interpretación del artículo 30 LOPDP de acuerdo con el artículo 4 de la misma Ley. Hay que recordar que el Reglamento General de Protección de Datos, en los principios relativos al tratamiento, establece que los datos personales serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente para fines incompatibles (limitación de la finalidad, artículo 5).

Todo ello queda perfectamente reflejado en las resoluciones de la Agencia Española de Protección de Datos. Muestra de ello es la resolución 495/2004: se había publicado en diferentes medios de comunicación con formato de publicidad un documento cuyo contenido, en esencia, consistía en recoger datos de personas físicas, quienes

habían de enviar su petición para que se gestionara en un apartado de correos, fax o correo electrónico. El interesado tenía que seleccionar siete deseos de una lista de treinta y tres que definían de una u otra manera un determinado perfil de la persona. Por su parte, una asociación de consumidores afirmaba que el consentimiento otorgado era nulo ya que la información suministrada al interesado no permitía conocer la auténtica finalidad a la que se iban a destinar los datos. En el cupón aparecía la siguiente cláusula: «[...] la empresa XXX podrá ceder sus datos a empresas del sector del marketing (*gadgets* y hogar, editoriales, ocio y pasatiempos, moda, cosmética y gran consumo, publicidad directa, seguros, telecomunicaciones, etc.) para enviarle publicidad de otros productos que puedan ser de su interés». La AEPD estableció que, de acuerdo con las exigencias del artículo 5 LOPDP, estas informaciones eran incompletas. Las expresiones «*gadgets*, publicidad directa, etc.», por el desconocimiento del concepto o por la amplitud de categorías de bienes y servicios a los que pudieran referirse, no permitían al afectado identificar de forma determinada y explícita las finalidades para las que serían tratados sus datos personales, en términos que le permitieran prestar un consentimiento inequívoco como el exigido por la LOPDP.

En esta resolución se afirmaba que la cláusula informativa «tras incorporar algunas finalidades determinadas, las combina con conceptos de difícil comprensión y, sobre todo, incorpora una finalidad –publicidad directa– que por generalidad e indeterminación podría comprender cualquier clase de bienes o servicios, a la que se añade la expresión "etc.", que pretendería ampliar el consentimiento a cualquier tipo de actividad». Se condenaba a esta empresa al pago de una multa de 6.000 euros.

Técnicas fraudulentas

También hay determinadas técnicas fraudulentas. Es el caso que se plantea en la resolución de la AEPD de archivo de actuaciones, «Expediente Nº: E/03597/2016» (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/archivo_actuaciones/archivo_actuaciones_2017/common/pdfs/E-03597-2016_Resolucion-de-fecha-12-05-2017_Art-ii-culo-6-LOPD.pdf): «Tras estudiar el patrón que se repetía en esas altas fraudulentas, detectaron que se realizaban a través del canal e-marketing de la entidad Clicktron Media y habían sido procesados por un robot. Inmediatamente desactivaron la colaboración con la entidad mencionada y han puesto un sistema "kaptcha" en los sitios en los que se promocionan para evitar que un robot introduzca altas fraudulentas de forma automática. También denunciaron los hechos ante la Policía Nacional».

5.2.4. Comunicaciones comerciales electrónicas: LSSICE-LOPDP y la relación contractual previa

Hoy en día es muy frecuente que el envío de comunicaciones comerciales se haga por vía electrónica como ya se ha establecido en el punto anterior al que nos remitimos. En este caso hay que acudir, además de a la normativa sobre protección de datos, a la de comercio electrónico, la LSSICE. Las normas referentes a la contratación a distancia, tanto la general como la de comercialización a distancia de servicios financieros, remiten a esta Ley. En el caso de la contratación a distancia, con carácter general, afirma el artículo 94 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, que:

«En las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica y en la contratación a distancia de bienes o servicios por medios electrónicos se aplicará, además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información y comercio electrónico. Cuando lo dispuesto en este título entre en contradicción con el contenido de la normativa específica sobre servicios de la sociedad de la información y comercio electrónico, esta será de aplicación preferente.»

Y según el artículo 96.4:

> «En todo caso, deberán cumplirse las disposiciones vigentes sobre protección de los menores y respeto a la intimidad. Cuando se utilicen datos personales procedentes de fuentes accesibles al público para la realización de comunicaciones comerciales, se proporcionará al destinatario la información que señala la Ley Orgánica de Protección de Datos de Carácter Personal, y se ofrecerá al destinatario la oportunidad de oponerse a la recepción de las mismas.»

En sentido muy parecido, el artículo 14 de la Ley 22/2007, de 11 de julio, de comercialización a distancia de servicios financieros destinados a los consumidores, remite a lo dispuesto en la Ley General de Telecomunicaciones y en la LSSICE.

El artículo 19 LSSICE deja muy clara la relación entre las dos leyes: LSSICE-LOPDP. Según su apartado segundo:

> «En todo caso, será de aplicación la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.»

Respecto a las comunicaciones comerciales por vía electrónica, deberán ser claramente identificables como tales y se deberá identificar a la persona física o jurídica en nombre de la cual se realizan. El artículo 21 LSSICE, ya mencionado anteriormente, es el encargado de prohibir el envío de comunicaciones comerciales no solicitadas, estableciendo el sistema conocido como *opt in*: queda prohibido el envío de comunicaciones publicitarias o promocionales que no hubieran sido previamente solicitadas o expresamente autorizadas por los destinatarios de las mismas. Es decir, hará falta el consentimiento previo del interesado. El carácter de este precepto de la LSSICE es todavía más restrictivo que la LOPDP y su reglamento de desarrollo, ya que no podrán enviarse comunicaciones comerciales sin el previo consentimiento del afectado ni siquiera en el caso de que los datos provengan de fuentes accesibles al público.

La resolución de la AEPD 317/2006 es clara en este sentido: «La cuestión es que este procedimiento no se inicia por una presunta vulneración de la LOPDP, sino de la LGT, y esta Ley no establece ningún tipo de exención al consentimiento previo e informado en los envíos de fax con fines de venta directa por haberse obtenido los datos de fuentes accesibles al público a tenor de la citada Ley Orgánica». En este caso, se vulneraba el artículo 38.3 LGT según el cual los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos: «h) a no recibir llamadas automáticas sin intervención humana o mensajes de fax con fines de venta directa sin haber prestado su consentimiento previo e informado para ello».

Se planteó otra interesante cuestión frente a la AEPD respecto a la obtención del consentimiento. Se discutía si la entrega de una tarjeta de visita en el marco de una feria en el ámbito de las nuevas tecnologías se podía entender como consentimiento para el tratamiento de los datos contenidos en la misma. La

AEPD, en su resolución 117/2005, entendía que no era suficiente este hecho como tal consentimiento. Sin embargo, los tribunales han fallado en sentido contrario.

Además, con carácter general, el destinatario podrá revocar en cualquier momento el consentimiento prestado para la recepción de comunicaciones comerciales. Para ello, se deberán prever procedimientos sencillos y gratuitos. Además, se deberá facilitar información accesible por medios electrónicos sobre dichos procedimientos.

Pero lo establecido en el artículo 21 LSSICE que se está comentando choca con lo dispuesto en el artículo 15 RDLOPD, cuyo apartado 15.1 dice:

> «Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste su negativa al tratamiento o comunicación de datos.»

En el caso de comunicaciones comerciales por vía electrónica, se refiere a supuestos que no encajan con la excepción del artículo 21 y, como ya ha quedado apuntado, aquel es el único supuesto en el que se pueden enviar estas comunicaciones sin el consentimiento previo del consumidor. Este artículo invertiría la regla hacia el sistema *opt out*.

En el caso de comunicaciones comerciales por otros medios de comunicación, debe analizarse el artículo 15 RDLOPD junto con el artículo 6 LOPDP. Según este último artículo, no será necesario el consentimiento del afectado para el tratamiento de datos de carácter personal cuando los datos se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y «sean necesarios para su mantenimiento o cumplimiento».

5.2.5. Tratamiento de datos en campañas publicitarias: entidades implicadas y delimitación de responsabilidades

Según el artículo 46 RDLOPD, para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes, será preciso que el tratamiento se ampare en alguno de los supuestos del artículo 6 LOPDP (es decir, consentimiento o las excepciones contenidas en este precepto). De nuevo nos encontramos ante un ámbito restrictivo: «entre sus clientes». Hay que tener en cuenta que son muchas las resoluciones de la AEPD sobre esta materia que condenan, precisamente, por infracción del artículo 6 LOPDP.

Pero, además, una determinada entidad puede contratar o encomendar a terceros la realización de una campaña publicitaria de sus productos o servicios, lo que suele ser habitual en la práctica. A ello se refiere el artículo 46 en sus

apartados 2, 3 y 4. En este caso, las principales cuestiones que surgen son: qué hay que entender por «parámetros identificativos», por una parte, y la determinación de responsabilidades, por otra.

Según el artículo 46.4 RDLOPDP y a los efectos previstos en el artículo 46, 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». Como se ve, es una definición muy amplia. Con esta definición cabrían, como parámetros identificativos de una determinada campaña, algunos como «jóvenes de entre 18 y 25 años», «hombres/mujeres de entre 25 y 35», etc.

Para la delimitación de responsabilidades se establecen las siguientes reglas:

- Cuando la entidad que contrate la campaña fije los parámetros identificativos de los destinatarios de la misma, esta será responsable del tratamiento de los datos.

- Cuando los parámetros identificativos sean determinados únicamente por la entidad o entidades contratadas, serán responsables del tratamiento estas entidades.

- Cuando ambas entidades intervengan en la determinación de los parámetros identificativos, ambas serán responsables del tratamiento.

Pero, además, es la entidad que encargue la campaña sobre la que recae la necesidad de asegurarse de que la entidad contratada ha actuado de acuerdo con la LOPDP y tiene que hacerlo «con la debida diligencia». Es decir, no basta encargar a otra empresa la campaña publicitaria, sino que además debe asegurarse de que esta recoge los datos correctamente. Es decir, ambas serían responsables y el encargo no le exime de responsabilidad.

En la resolución 533/2005 de la AEPD, el señor XYZ recibió una oferta publicitaria de Directel, habiendo sido suministrados sus datos personales por la empresa Relacional sin que el señor XYZ hubiera dado su consentimiento. Directel se dedica exclusivamente a recibir llamadas de potenciales clientes, para lo cual contrata los servicios de empresas que le realizan la campaña publicitaria, incluida la obtención de datos de los destinatarios. Entre ambas empresas hay un contrato de prestación de servicios para la realización de la campaña publicitaria del año 2003. Los datos debían ser recabados por Relacional, de acuerdo con la LOPDP y siempre de listados de acceso al público. Relacional es la única propietaria de los ficheros y la que lleva a cabo el tratamiento de los mismos. El beneficiario de la campaña es Directel. Pero en este caso, los datos del señor XYZ no se han obtenido con su consentimiento ni provienen de una fuente accesible al público. También se refiere al censo promocional previsto en la LOPDP, pero aún no se ha iniciado su elaboración. Se condena a las dos empresas por vulneración del principio del consentimiento (artículo 6 LOPDPD) y no concurrir las causas de exclusión del consentimiento del apartado 2º del artículo 6 LOPDP. Además, esta resolución añade que la actuación de Directel supone una «falta de diligencia debida que le era exigible y que ha provocado el tratamiento de los datos del denunciante sin su consentimiento».

En sentido parecido se expresa la resolución 580/2005. En este caso, Mirvak solicitó a Ofertas Vivas la remisión de aproximadamente 10.000 envíos publicitarios a direcciones de Barcelona. El denunciante recibe uno de estos envíos. Según se afirma en esta resolución, el sistema de protección que perfila la LOPDP resulta exigible a Mirvak. Esta empresa debió verificar de forma diligente que el tratamiento de datos se hacía conforme a las exigencias del artículo 6 LOPDP. Muy similar es la resolución 604/2005.

Y en la resolución 249/2005, DIRECTEL, como beneficiaria de la campaña, es responsable del tratamiento de los datos personales utilizados en la misma. Por ello, ha cometido la infracción prevista en el artículo 44.3.d), dado que el tratamiento de los datos del denunciante se efectuó sin contar con su consentimiento y sin que se diera ninguna de las causas de exclusión del consentimiento contempladas en el artículo 6.2 de la citada Ley Orgánica, vulneración del principio de consentimiento.

Las relaciones entre las distintas entidades implicadas en una campaña publicitaria también las tiene en cuenta el Reglamento para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, que se estudiarán más adelante.

En otra sede, esta vez más general, de relaciones entre empresas se puede situar el artículo 47 RDLOPDP referido a la depuración de datos personales. Regula el supuesto en el que dos o más responsables, ya sea por sí mismos, ya sea por encargo a terceros, pretendieran, sin consentimiento de los afectados, constatar quiénes ostentan la condición de clientes de una u otra o de varios de ellos, con fines de promoción o comercialización de sus productos. El tratamiento así realizado constituirá una cesión o comunicación de datos. La reflexión que se plantea es: aun no existiendo este artículo, ¿no estaríamos ante una cesión o comunicación de datos del artículo 11 LOPDP?

5.2.6. Ficheros de exclusión: control de los datos contenidos en estos ficheros

Los artículos 48 y 49 RDLOPDP se refieren, el primero, a los ficheros de exclusión y, el segundo, a los ficheros comunes de exclusión. Según el primero de estos artículos, los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad. El principal problema será precisamente determinar en qué consisten estas «medidas necesarias».

Formas de exclusión

En el artículo 31.3 LOPDP encontramos una referencia a formas de exclusión, esta vez, del censo promocional. Este artículo establece, respecto al censo promocional, que se regularían reglamentariamente los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional. Estos procedimientos han de ser gratuitos para los interesados y trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de las personas que así lo hayan solicitado.

Por otra parte, se podrán crear ficheros comunes de exclusión de carácter general o sectorial. Serán objeto de tratamiento los datos necesarios para evitar el envío de comunicaciones comerciales a aquellas personas que así lo hayan solicitado. Solo podrán contener los datos mínimos imprescindibles. El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en estos ficheros comunes. La entidad responsable, por supuesto, debe cumplir con lo establecido en la LOPDP.

Dada la finalidad de estos ficheros de exclusión, los datos a conservar serán los mínimos para identificar a la persona que ha manifestado su negativa a recibir publicidad. El tema de los ficheros de exclusión no está exento de problemas, que se multiplican en el ámbito de la gestión de los mismos, destacando entre los principales el de saber quién debe ser el responsable de estos ficheros (¿Debería ser una entidad privada o una entidad pública?). Conseguir que estos ficheros sean eficaces va a ser el punto clave para que cumplan la finalidad a la que están destinados. Habrá que buscar las medidas adecuadas para que se cumpla su finalidad. Para conseguir que sean eficaces es necesaria su actualización y, precisamente, que en la práctica sean consultados por aquellas empresas que llevan a cabo campañas publicitarias (así lo exige el apartado 4º del artículo 49 del RDLOPDP).

En la resolución 21/2006 se resuelve el siguiente supuesto: don XYZ se dirigió a la entidad Datasun para verificar el origen de los datos utilizados por esa entidad para la remisión de correos publicitarios. El denunciante no figura en las páginas blancas disponibles en Internet. Don XYZ ejercita su derecho de acceso. Se le informa de las listas Robinson y envía un fax para que le incluyan en la mencionada lista. Pero en fecha posterior recibe un nuevo envío publicitario en su domicilio. Se sanciona a Datasun por infracción grave por vulneración del artículo 6.1 LOPDP. A pesar de ello, lo que queda patente es la falta de eficacia, en este caso, de las denominadas «listas Robinson».

Y la resolución 412/2017, contra la entidad Trendlearning, S.L., también establece la obligación de consultar las listas Robinson. Afirma la resolución que:

«Por tanto, y aun considerando que los datos personales del denunciante constaban en una fuente de acceso público, lista de personas que pertenecen a un grupo profesional, y que dicha circunstancia opera como excepción a la prestación del consentimiento, no puede obviarse un elemento fundamental, que los datos personales del denunciante figuran inscritos en un fichero general de exclusión de acciones comerciales y publicitarias y debió haber sido consultado antes de realizar la llamada.

Por último, hay que señalar que el tenor literal del artículo 6 LOPD señala claramente que: "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa". Por ello, de conformidad con lo previsto en las normas transcritas, los datos personales del denunciante debieron ser excluidos de las acciones publicitarias realizadas por la entidad denunciada.»

También en este sentido apunta la resolución de la AEPD 437/2017, contra la entidad Saber y Agua Pura, S.L.U.:

«En el supuesto examinado, los datos personales del denunciante fueron utilizados con fines publicitarios y sin su consentimiento. Se ha acreditado que SABER y AGUA no tenía el consentimiento del denunciante para el tratamiento de sus datos, no concurriendo ninguno de los supuestos que dispensen a este y legitimen el tratamiento de datos denunciado, esto es, la utilización del dato personal del denunciante relativo al número de la línea de telefonía para la realización de llamadas promocionales con posterioridad a la fecha en la que tales datos se registraron en el fichero de exclusión de Adigital.»

En la resolución 1145/2017 (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2017/common/pdfs/PS-00570-2016_Resolucion-de-fecha-16-05-2017_Art-ii-culo-30.4-6.1-LOPD.pdf) se expone un procedimiento sancionador de la AEPD frente a la empresa Orange Espagne, S.A.U., en la que se archivan las actuaciones contra esta empresa. En este caso, don A.A.A. denuncia que recibe reiteradamente llamadas publicitarias de Jazztel y Orange Espagne, SAU, en su número de teléfono. El denunciante aporta copia de correo electrónico de fecha 25 de noviembre de 2015 en el que Jazztel le contesta a su solicitud de derecho de oposición y le informa de la exclusión de sus datos con fines publicitarios, pero con posterioridad sigue recibiendo llamadas publicitarias. La resolución afirma que:

«Uno de los pilares básicos de la normativa reguladora del tratamiento automatizado de datos es el principio del consentimiento o autodeterminación, cuya garantía estriba en que el afectado preste su consentimiento consciente e informado para que la recogida de datos sea lícita. Se trata de una garantía fundamental legitimadora del régimen de protección establecido por la Ley, en desarrollo del artículo 18.4 de la Constitución Española, dada la notable incidencia que el tratamiento automatizado de datos tiene sobre el derecho a la privacidad en general, y que solo encuentra como excepciones al consentimiento del afectado aquellos supuestos que, por lógicas razones de interés general, puedan ser establecidos por una norma con rango de ley.»

El Anteproyecto de Ley de Protección de Datos de Carácter Personal incluye un artículo dedicado a los sistemas de exclusión publicitaria que establece la licitud del tratamiento de datos con el fin de evitar el envío de comunicaciones comerciales a quienes se hubieran opuesto a ello. La cuestión se regula en los siguientes términos:

«1. Será lícito el tratamiento de datos de carácter personal que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados.

2. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados con fines de publicidad o prospección comercial, este deberá informarle de los sistemas de exclusión publicitaria existentes, identificando a su responsable.

3. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo.

4. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán su creación, su carácter general o sectorial y el modo en que los afectados pueden incorporarse a los mismos a la Agencia Española de Protección de Datos, que hará pública la citada información.»

5.2.7. Derechos de acceso, rectificación, cancelación y derecho de oposición

En relación a los derechos de acceso, rectificación y cancelación (artículo 50 RDLOPDP), hay que remitirse a lo dispuesto en los capítulos I a IV del Título III del Reglamento que desarrolla la LOPDP y, con carácter general, a la LOPDP. Para que el afectado pueda ejercer estos derechos, debe tener conocimiento de que sus datos de carácter personal se van a utilizar para fines publicitarios o de prospección comercial. De ahí nuevamente la importancia de las finalidades a las que se destinan los datos, tema ya tratado en un apartado anterior.

El RDLOPDP se preocupa especialmente de las relaciones entre las distintas empresas implicadas, por ejemplo, para las campañas publicitarias, que en la práctica es muy frecuente. Por ello, según el artículo 50.2 RDLOPDP, si una determinada entidad ha encargado la campaña a un tercero:

- La primera está obligada en el plazo de diez días, desde la recepción de la comunicación de la solicitud del ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero.

- El responsable del fichero tiene que otorgar al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Con una redacción bastante confusa, el artículo 50 RDLOPD establece que todo ello se entenderá sin perjuicio del deber impuesto en el párrafo segundo del artículo 5.5 LOPDP.

Artículo 5.5 LOPDP

Afirma este artículo: «Asimismo, tampoco regirá lo dispuesto en el párrafo anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten».

Respecto al derecho de cancelación, la resolución de la AEPD 722/2004 resuelve el siguiente supuesto: don A.R.V., tras recibir en su domicilio una comunicación remitida por Telyprom, donde se indica que sus datos han sido facilitados por la sociedad Datasun, ejerció el derecho de cancelación. Recibe la siguiente respuesta: «No podemos acceder a su petición ya que sus datos personales no figuran en fichero alguno propiedad de Datasun, ya que Datasun para prestar sus servicios utiliza las bases de sus clientes. No obstante, y a efectos de poder ejercitar sus derechos, le rogamos se ponga en contacto con la empresa de la cual recibió publicidad o nos remita o comunique el contenido del envío publicitario para poder ponernos en contacto con dicha empresa y transmitirle su petición». Así lo hizo, contestándole: «nos pondremos en contacto con la empresa publicitaria para que cancelen sus datos y no se reciba ningún tipo de publicidad por su parte». Después, don A.R.V. recibió una nueva comunicación comercial procedente de Telyprom con datos de la empresa Datasun. Se ejerce el derecho de cancelación en dos ocasiones, pero el denunciante continúa recibiendo anuncios publicitarios en los que consta que los datos del destinatario proceden de Datasun. Se condena a esta empresa por una infracción del artículo 6 y el artículo 15 de la LOPDP. Por otra parte, en la resolución 354/2006 la empresa en cuestión infringió lo dispuesto en el artículo 16 en relación con el 30.4 LOPDP, puesto que no canceló en sus ficheros los datos de la denunciante tras la solicitud de esta.

El artículo 51 RDLOPDP se refiere al derecho de oposición que tienen todos los interesados. Las consecuencias del ejercicio de este derecho son claras: serán dados de baja del tratamiento, cancelándose las informaciones que se tengan sobre ellos, a su simple solicitud.

Hay que tener en cuenta que este derecho de oposición se entiende sin perjuicio del derecho del interesado a revocar su consentimiento para el tratamiento de los datos cuando lo estime oportuno.

Resolución R/01232/2017 de la AEPD (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2017/common/pdfs/PS-00069-2017_Resolucion-de-fecha-10-05-2017_Art-ii-culo-6-LOPD.pdf). En el procedimiento sancionador frente a la Federación de Servicios Públicos de La Unión General de Trabajadores (FSP-UGT):

«El presente procedimiento tiene por objeto el examen de la denuncia formulada por el tratamiento realizado por la entidad FSP-UGT de los datos personales del denunciante, concretamente el relativo a su dirección de correo electrónico, en contra de la voluntad expresa del mismo, que había manifestado a aquella entidad su oposición a dicho tratamiento de datos. Consta acreditado en las actuaciones que el denunciante, según el detalle reseñado en los Hechos Probados, se dirigió a la entidad imputada mediante correo electrónico de fecha 13 de enero de 2016, desautorizando expresamente la comunicación vía correo electrónico y solicitando, en definitiva, que cesara la utilización de su dato personal relativo a la dirección de correo electrónico.

En las actuaciones consta igualmente acreditado que la entidad FSP-UGT recibió dicho correo del denunciante y lo contestó. Cabe decir, por tanto, que la entidad FSP-UGT no contaba con el consentimiento del denunciante para el tratamiento de datos personales realizado, en concreto, la utilización de su dirección de correo electrónico, con ningún fin, incluido el de remitir información sindical.

Por otro lado, FSP-UGT alega que para remitir información al conjunto de los trabajadores utiliza la lista de distribución facilitada, en este caso, por el Ayuntamiento de Madrid. Este hecho implica que la entidad reclamada no necesita el consentimiento previo del afectado para el tratamiento de sus datos, ahora bien, una vez recibida la solicitud de oposición del reclamante, la entidad deberá proceder a atender el deseo expresado por el interesado, dado que el envío de correos electrónicos utilizando la lista de distribución referida implica un tratamiento de los datos, lo que convierte a FSP-UGT en responsable del tratamiento, teniendo la obligación de atender los derechos ARCO recogidos en la normativa vigente en materia de protección de datos.

En consecuencia, se estima vulnerado por la entidad imputada el artículo 6.1 de la LOPD, en relación con el artículo 16.1 de la misma norma, considerando que la entidad FSP-UGT infringió la normativa de protección de datos personales en el sentido expuesto, al no hacer efectivo el deseo del denunciante de oponerse a recibir comunicaciones de aquella entidad remitidas mediante correo electrónico a la dirección señalada expresamente por el denunciante, así como a la cancelación de sus datos personales. La entidad FSP-UGT, sin contar con el consentimiento del denunciante, ha efectuado un tratamiento de los datos personales del mismo que vulnera el principio del consentimiento recogido en el artículo 6 de la LOPD.»

En la Resolución R/01248/2017 (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2017/common/pdfs/TD-02394-2016_Resolucion-de-fecha-03-05-2017_Art-ii-culo-34-RD-1720-b-2007.pdf), en reclamación formulada por don A.A.A. contra la entidad Orange España Virtual, S.L., se estima la reclamación formulada por no haber atendido la empresa reclamada el derecho de oposición de don A.A.A., a los efectos de no recibir más comunicaciones comerciales, de acuerdo con el artículo 30 LOPDP.

Si ya han quedado planteadas las consecuencias del ejercicio del derecho de oposición, ahora corresponde analizar los medios para llevarlo a cabo. Del artículo 50.2 RDLOPDP se extrae que este derecho tiene que ejercitarse previa petición y sin gastos mediante un procedimiento sencillo y gratuito de oposición. A ello se le tendría que añadir «y adecuado a la técnica de comunicación utilizada» –algo que no aparece en el artículo.

El Reglamento se encarga de enumerar, tanto en sentido positivo como en sentido negativo, algunos ejemplos. Se puede ejercitar mediante la llamada a un número de teléfono gratuito o la remisión de un correo electrónico. También podrá utilizarse el teléfono de atención al cliente o el de reclamaciones si la entidad en cuestión lo tuviera; eso sí, no hay que olvidar que no puede suponer un coste para el afectado. En cambio, no podrán exigirse cartas certificadas o utilización de servicios de telecomunicaciones que supongan tarificación adicional al afectado u otros que supongan un coste específico. No puede suponer un ingreso adicional para el responsable del tratamiento.

El artículo 22.2 LSSICE se refiere a los dispositivos de almacenamiento y recuperación de datos en equipos terminales (entre ellos, *spyware*, *web bugs*, etc.). En este caso, se tiene que informar a los destinatarios de manera clara y completa de su utilización y finalidad, ofreciéndoles, también, la posibilidad de rechazar el tratamiento de los datos mediante un «procedimiento sencillo y

gratuito de oposición». En estos casos, el tema del procedimiento de oposición es más complicado cuando a veces los usuarios no son ni siquiera conscientes de su existencia y hace falta un software específico para detectarlos.

¿Ante quién puede el afectado ejercitar su derecho de oposición cuando hay más de una empresa implicada en la campaña publicitaria? Igual que en el caso de los derechos de acceso, rectificación y cancelación, si hay dos entidades implicadas, la entidad que hubiera encargado la campaña a un tercero estará obligada, en el plazo de 10 días desde la recepción de la comunicación de la solicitud del ejercicio del derecho de oposición, a comunicárselo al responsable del fichero. Este deberá atender el derecho del afectado en el plazo de 10 días desde la recepción de la comunicación. Como en el caso anterior, todo ello se entiende sin perjuicio de lo dispuesto en el artículo 5.5, apartado segundo, de la LOPDP.

Referencias bibliográficas

P. Grimalt Servera (2005). «Deberes y responsabilidades en materia de protección de datos». En: Cavanillas Múgica, S. (coord.) *Deberes y responsabilidades de los servicios de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares (págs. 183-201).

A. Paniza Fullana (2004). «Comunicaciones comerciales no solicitadas y marketing directo: el sistema *opt-out* como excepción. Correo electrónico y mensajes SMS con fines publicitarios». En: *Avances en Criptografía y Seguridad de la Información*. Madrid: Díaz de Santos (págs. 437-445).

5.3. El uso de los datos de geolocalización

También especialmente interesante para la protección de la privacidad del usuario o consumidor en sentido amplio es el uso de datos de geolocalización por parte de los prestadores de servicios de la sociedad de la información. La publicidad que puede conseguirse con el uso de estos datos también es especialmente interesante para los prestadores de servicios.

La regulación sobre esta materia ya se encuentra en el artículo 9 de la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas), transpuesto a nuestro ordenamiento en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Concretamente, en su artículo 38.3 establece que:

> «En particular los abonados a los servicios de comunicaciones electrónicas tendrán los siguientes derechos: d) a que solo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.»

En consecuencia, tienen que ser datos o bien recogidos de forma anónima o con consentimiento del usuario.

Lectura recomendada

Sobre la anonimización, véase:

Grupo de Trabajo del Artículo 29 (2014, 10 de abril). «Dictamen 05/2014 sobre técnicas de anonimización». Disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf.

Es decir, para poder utilizar estos datos de localización, que pueden ser especialmente interesantes en determinadas campañas de publicidad, tienen que cumplirse los requisitos exigidos por esta norma. Así se establece en el Informe de la Agencia de Protección de Datos 160/2004 sobre el nivel de seguridad de ficheros con datos de localización:

> «Suponiendo que el tratamiento de los datos cumpla con los requisitos que se han señalado anteriormente, dicho tratamiento permitiría conocer la localización del afectado en cada momento concreto o en los supuestos en que dicha localización fuera sometida a tratamiento, lo que supondrá un conocimiento suficiente del comportamiento del usuario de la terminal sometida a localización, en caso de que dicho usuario fuera suficientemente identificable.»

La propia definición de **dato de carácter personal** en el Reglamento General de Protección de Datos ya se refiere a los datos de localización: «toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». La posibilidad de muchas aplicaciones móviles de ofrecernos servicios cercanos al lugar donde estamos personaliza todavía más la publicidad que nos ofrecen.

La Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas también se refiere a los datos sobre la ubicación del dispositivo. Esta propuesta define los **metadatos de comunicaciones electrónicas** como: «datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; se incluyen los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación».

Sobre los datos de localización es interesante el documento «Best Practices and Guidelines for Location-Based Services» de The Wireless Association (disponible en: http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf), que se refiere a los datos de localización en este sentido:

«First, LBS Providers must inform users about how their location information will be used, disclosed and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure.

Second, once a user has chosen to use an LBS, or authorized the disclosure of location information, he or she should have choices as to when or whether location information will be disclosed to third parties and should have the ability to revoke any such authorization.

LBS Providers must inform LBS users about how their location information will be used, disclosed and protected

LBS Providers may use written, electronic or oral notice so long as LBS users have an opportunity to be fully informed of the LBS Provider's information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous.

- **Form of consent**.

- **Revocation of consent**: LBS Providers must allow LBS users to revoke their prior consent to disclose location information to all or specified third parties.

- **Protection of minors**.»

Lectura recomendada

Sobre esta cuestión, véase:

M. Payeras Capellà; M. Mut Puigserver; A. Paniza Fullana; A. P. Isern Deyà (2014). «Privacidad en servicios turísticos basados en geolocalización». *Revista de Derecho, Empresa y Sociedad* (REDS) (núm. 5, ISSN: 2340-4647, págs. 78-93).

5.4. Redes sociales y publicidad

En el «Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online» de la Agencia Española de Protección de Datos (disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf), se plantean diferentes riesgos para la privacidad, entre otros:

- El uso de redes sociales como plataformas para el envío de correos electrónicos no solicitados.

- La publicidad hipercontextualizada, si bien puede suponer una ventaja para los usuarios, ya que solo recibirán aquella publicidad sobre contenidos que les interesen, descartando otros que resultarían irrelevantes, no hay que olvidar de qué forma se ha conseguido esta información. Para poder contextualizar la publicidad se tienen que rastrear los datos y las preferencias de los usuarios. Ello nos puede llevar al uso de *cookies*, sin el conocimiento del usuario, que permitan a la plataforma conocer cuál es la actividad del usuario dentro de la misma.

Ejemplo: Facebook

«Es posible que Facebook utilice información de tu perfil sin identificarte individualmente ante terceros. Esto se hace con propósitos como establecer a cuánta gente en una red le gusta un grupo o una película, y para personalizar anuncios y promociones. Creemos que esto es beneficioso para ti puesto que te permite estar mejor informado sobre lo que ocurre a tu alrededor. Y cuando aparecen anuncios, es más probable que sean de interés para ti. Por ejemplo, si pones una película que te gusta en tu perfil, podemos mandarte un anuncio sobre el estreno de otra del mismo estilo en tu ciudad. Sin embargo, no informamos a la productora cinematográfica de tu identidad.»

También es interesante el «Dictamen 5/2009 sobre las redes sociales en línea» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf), en el que, en relación con temas relacionados con la publicidad, se apunta:

«Los SRS pueden definirse generalmente como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información, según se definen en el artículo 1, apartado 2, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE. Los SRS comparten determinadas características:

- los usuarios deben proporcionar datos personales para generar su descripción o "perfil";

- los SRS proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios);

- las "redes sociales" funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que los usuarios pueden interactuar. Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información. Es por tanto importante que los SRS funcionen respetando los derechos y las libertades de los usuarios, que tienen la expectativa legítima de que los datos personales que revelan sean tratados de acuerdo con la legislación europea y nacional relativa a la protección de datos y de la intimidad.»

Lectura recomendada

Sobre esta cuestión, véase:

A. Troncoso Reigada (2012). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales». *Revista de Internet, Derecho y Política* (núm. 15, págs. 61-75).

6. La regulación de las *cookies*

6.1. Las *cookies* y otros instrumentos de navegación: concepto y clases

No puede olvidarse que la tecnología avanza muy rápidamente y, junto a las conocidas *cookies* y otros instrumentos como los programas espía o *web bugs*, van apareciendo otras técnicas capaces de obtener información de los equipos de los usuarios. A ello se refiere la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, norma que modificará la regulación actual sobre *cookies* y otros instrumentos de navegación capaces de obtener datos e información del usuario: «también es posible recopilar a distancia información relacionada con el dispositivo del usuario final a efectos de identificación y seguimiento, utilizando técnicas como la "huella digital de dispositivo", con frecuencia sin el conocimiento del usuario final, lo cual puede suponer una grave intromisión para la privacidad de estos». Por ello, y tal y como afirma esta propuesta, las interferencias de este tipo en el equipo terminal del usuario final solo se pueden permitir con el consentimiento del usuario y para fines específicos y transparentes. Las excepciones deben limitarse a situaciones que no entrañen intromisión, o que esta sea muy limitada, en la vida privada

¿Qué son las ***cookies?*** Son cadenas de información alfanumérica que el servidor deposita en el disco duro del ordenador del usuario durante una visita al mismo. Esto posibilita su reconocimiento en visitas posteriores.

Se distinguen distintos tipos de *cookies*. Las *cookies* anónimas, que no incluyen un campo identificador único para cada usuario, a diferencia de las *cookies* identificadas, con las que se pueden relacionar accesos de usuario y crear perfiles cada vez más completos del usuario. También se pueden diferenciar las *cookies* temporales, que desaparecen cuando se cierra el navegador, y las *cookies* persistentes, que permanecen como archivo en el ordenador del usuario cuando se cierra el navegador.

Otro tipo más específico son las *cookies* en *flash* (*local shared objects*), que se almacenan en el disco duro del usuario a través de aplicaciones de *flash* al visitar un determinado sitio web. Tienen mayor capacidad de almacenamiento y plantean más dificultades cuando se quieren eliminar.

Ejemplo:

Fuente: http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html.

A continuación se plantean ejemplos de la información sobre *cookies* de diferentes sitios web. En ellos se ven los distintos tipos de *cookies* utilizados así como las diferentes políticas establecidas para su uso. Se resaltan en negrita algunos párrafos que nos servirán para reflexionar sobre la aplicación de la normativa:

Rumbo.es

La Sociedad recogerá tus datos personales, como usuario y/o cliente, a través de las siguientes fuentes:

- Directamente de ti porque los facilitas directamente a la Sociedad rellenando y enviando el formulario de registro en cualquiera de los servicios de la Sociedad, a través del sitio web o telefónicamente a nuestro Servicio de Atención al Cliente. Son datos como el nombre, los apellidos, el correo electrónico, el número de teléfono, etc., necesarios para la prestación de los servicios solicitados a la Sociedad.

- A través de sistemas informáticos y procedimientos de software presentes en el sitio web para garantizar su correcto funcionamiento que, implícitamente, en su normal ejercicio, utilizan protocolos de comunicación de Internet. Se trata de información que no se recoge para ser asociada contigo, pero que, por su propia naturaleza, podría permitir identificarte. En esta categoría de datos están las direcciones IP o los nombres de dominio de los ordenadores que se conectan al sitio web, las direcciones de URI (*uniform resource identifier*) de las solicitudes realizadas, el horario de la solicitud, el método utilizado para someter la solicitud al servidor, la dimensión del archivo obtenido como respuesta, el código numérico indicando el estado de la respuesta dada por el servidor (correcta, error, etc.) y otros parámetros relativos al sistema operativo y al ambiente informático utilizado. Estos datos se utilizan solo para recopilar información estadística anónima sobre el uso del sitio web y para controlar su correcto funcionamiento. Los datos podrían ser utilizados para comprobar la responsabilidad en caso de hipotéticos delitos informáticos y/o daños al sitio web.

- A través de la utilización de *cookies* en el sitio web. Las *cookies* constituyen información que a menudo contiene un código de identificación único anónimo, que es enviada al navegador por un servidor web y que queda almacenada en el disco duro de tu ordenador, *smartphone* o tableta (en adelante, "dispositivo"). Más tarde, y en el caso de que realices conexiones posteriores con el sitio web, las *cookies* pueden leerse y ser reconocidas por el sitio web que las envió. Se utilizan principalmente para hacer funcionar o mejorar el funcionamiento del sitio web,

así como para proporcionar información comercial y de marketing al propietario del sitio web.

De conformidad con el aviso de *cookies* que aparece en la *home page* del sitio web y con la presente política de *cookies*, aceptas que, al navegar por el sitio web, consientes expresamente el uso de *cookies* según lo aquí descrito, excepto en la medida que hayas modificado la configuración de tu navegador para rechazar la utilización de las mismas. A título enumerativo y no limitativo, se entiende que estás navegando por el sitio web al realizar alguna de las siguientes acciones: cerrar el aviso de *cookies* de la *home page*, desplazarte por el sitio web, hacer clic en cualquier elemento del sitio web, etc. A continuación se describen los tipos de *cookies* utilizados en el sitio web.

Tipos de *cookies* según la entidad que las gestiona

En función de quién sea la entidad que gestione el equipo o dominio desde donde se envían las *cookies* y trate los datos que se obtengan, se distinguen:

- *Cookies* propias: son aquellas que se envían a tu dispositivo desde un equipo o dominio gestionado por nosotros y desde el que se presta el servicio que has solicitado.

- *Cookies* de terceros: son aquellas que se envían a tu dispositivo desde un equipo o dominio que no es gestionado por nosotros, sino por otra entidad que trata los datos obtenidos través de las *cookies*.

Tipos de *cookies* según el plazo de tiempo que permanecen activadas

Según el plazo de tiempo que permanecen activadas en el dispositivo, podemos distinguir:

- *Cookies* de sesión: son un tipo de *cookies* diseñadas para recabar y almacenar datos mientras accedes al sitio web. Estas *cookies* no quedan almacenadas en tu dispositivo cuando caduca la sesión o se cierra el navegador.

- *Cookies* persistentes: son un tipo de *cookies* en el que los datos quedan almacenados en tu dispositivo y pueden ser accedidos y tratados cuando abandonas el sitio web y cuando te vuelves a conectar a él durante un periodo determinado. La duración máxima de las *cookies* persistentes que utilizamos en el sitio web es de 2 años.

Tipos de *cookies* según su finalidad

Según la finalidad para la que se traten los datos obtenidos a través de las *cookies*, podemos distinguir entre:

- *Cookies* técnicas: son estrictamente necesarias para el funcionamiento del sitio web y esenciales para permitir la navegación por nuestro sitio web y para el uso de las diversas funcionalidades del mismo. Sin ellas no es posible utilizar los servicios de búsqueda, comparación y reserva u otros servicios disponibles en el sitio web.

- *Cookies* de personalización: se utilizan para facilitar la navegación en el sitio web, para recordar las opciones que has elegido en el mismo y proporcionar funcionalidades más personalizadas. En algunos casos podemos permitir que los anunciantes u otros terceros coloquen *cookies* en nuestro sitio web para proporcionar contenido y servicios personalizados. En cualquier caso, el uso de nuestro sitio web constituye la aceptación para el uso de este tipo de *cookies*. Si las *cookies* fueran bloqueadas, no podemos garantizar el buen funcionamiento del mismo.

- *Cookies* analíticas para actividad estadística y de medición del tráfico: recopilan información sobre el uso del sitio web, las páginas que se visitan y posibles errores que puedan ocurrir durante la navegación. También utilizamos estas *cookies* para reconocer el lugar de origen de las visitas a nuestro sitio web. Estas *cookies* no recopilan información que pueda identificarte. Cualquier información se recoge de forma anónima y se utiliza para ayudar a mejorar el funcionamiento del sitio web y con finalidades estadísticas. Por tanto, estas *cookies* no contienen datos de carácter personal. En algunos casos, algunas de estas *cookies* son gestionadas en nuestro nombre por cuenta de terceros, pero no se les permite usarlas para fines diferentes a los mencionados anteriormente.

- ***Cookies* para fines publicitarios y de re-marketing: se utilizan para recopilar información con el fin de que la publicidad sea más interesante para ti y para**

mostrar anuncios publicitarios sobre el sitio web o sobre sitios de terceros u otras campañas publicitarias online. La mayoría de estas *cookies* son "*cookies* de terceros", por lo que son *cookies* de entidades ajenas a nosotros y, debido al modo en que funcionan estas *cookies*, no tenemos acceso a las mismas ni somos responsables del funcionamiento ni de la finalidad de las mismas. A través de sus políticas de privacidad puedes obtener más información sobre el funcionamiento, la finalidad y el uso que hacen de las *cookies* estos terceros. Esta información se puede consultar en el listado de *cookies* disponible más adelante. Asimismo, podemos utilizar los servicios de terceras empresas para recopilar datos y/o publicar anuncios cuando visitas nuestro sitio web. Estas empresas suelen usar información de forma anónima y agregada (sin incluir, por ejemplo, tu nombre, dirección, dirección de correo electrónico o número de teléfono) sobre visitas a este sitio web y otros sitios web con el fin de proporcionarte anuncios sobre productos y servicios de tu interés.

- *Cookies* sociales: estas *cookies* permiten compartir nuestro sitio web y hacer clic en "Me gusta" en los sitios de redes sociales como Facebook, Twitter, Google+, YouTube, etc., e interactuar con el contenido de las distintas plataformas. Las condiciones de utilización de estas *cookies* y la información recopilada se regulan por la política de privacidad de la plataforma social correspondiente que puedes consultar a continuación.

Para conocer el listado de *cookies* que utilizan este sitio web, haz clic en http://flights.lastminute.com/content/en/our-cookies.html.

La información contenida en el listado de *cookies* anterior ha sido facilitada por las empresas terceras que generan las mismas. Estas empresas tienen sus propias políticas de privacidad, donde establecen sus propias declaraciones así como sistemas de desactivación aplicables.

La Sociedad no se hace responsable del contenido y la veracidad de las políticas de privacidad de terceros incluidas en esta política de *cookies*.

Debes tener presente que si las *cookies* de tu dispositivo no están activadas, tu experiencia en el sitio web puede ser limitada e incluso podría impedir la navegación y la utilización de nuestros servicios.

Existen diversos modos de administrar las *cookies*. Mediante la modificación de la configuración del navegador puedes optar por desactivar las *cookies* o recibir un aviso antes de aceptar una. Asimismo, puedes borrar todas las *cookies* instaladas en la carpeta de *cookies* del navegador. Ten en cuenta que cada navegador tiene distintos procedimientos para gestionar su configuración. A continuación te explicamos cómo puedes gestionar las *cookies* por medio de los principales navegadores: [...].

Si deseas información sobre cómo gestionar *cookies* en tu tableta o *smartphone*, consulta la respectiva documentación o archivos de ayuda online.

Las *cookies* de terceros no las instalamos nosotros ya que son instaladas por nuestros socios comerciales u otros terceros cuando visitas este sitio web. Por tanto, te sugerimos que consultes los sitios web de esos terceros para obtener información sobre las *cookies* que instalan y cómo las puedes gestionar. No obstante, te invitamos a consultar la siguiente página web http://www.youronlinechoices.com/ donde encontrarás información útil sobre el uso de las *cookies* y sobre las medidas que puedes adoptar para proteger tu privacidad en Internet.

Google.com

Cookies y tecnologías similares:

«Tanto Google como nuestros partners utilizamos diferentes tecnologías para recoger y almacenar información cuando accedes a un servicio de Google, incluido el uso de *cookies* o tecnologías similares para identificar tu navegador o tu dispositivo. También utilizamos estas tecnologías para recoger y almacenar información cuando interactúas con servicios que ofrecemos a nuestros *partners* como, por ejemplo, servicios publicitarios o funciones de Google que pueden aparecer en otros sitios. Nuestro producto Google Analytics permite a las empresas y a los propietarios de sitios analizar el tráfico a sus sitios web y aplicaciones. Si se utiliza junto con nuestros servicios de publicidad, como los que utilizan la *cookie* de DoubleClick, el cliente de Google Analytics o Google vincula la información de Google Analytics, mediante la tecnología de Google, con la información sobre las visitas a diferentes sitios.»

Reflexión

¿Es lícito limitar e incluso impedir la navegación por un sitio web determinado si no aceptas las *cookies*? («Debes tener presente que si las *cookies* de tu dispositivo no están activadas, tu experiencia en el sitio web puede ser limitada e incluso podría impedir la navegación y la utilización de nuestros servicios».)

Analicemos ahora otros instrumentos de navegación que pueden captar y almacenar datos de los clientes.

La resolución de la AEPD: R/01753/2016 se refiere a un supuesto en el que se utilizaba la técnica del **enriquecimiento de cabeceras**. Afirma esta resolución que:

«El enriquecimiento de cabeceras es una funcionalidad utilizada únicamente en el protocolo HTTP que permite añadir meta-información a las peticiones de acceso a una página web concreta que se progresan desde el terminal del cliente hasta el servidor final. [...] algunos de los datos están definidos por el protocolo como información necesaria para establecer la comunicación, "x-up-subno" y "TMuser-id" son los introducidos por Telefónica como información necesaria para que Telefónica identifique al usuario y pueda gestionar las suscripciones a productos de Servicios Premium...

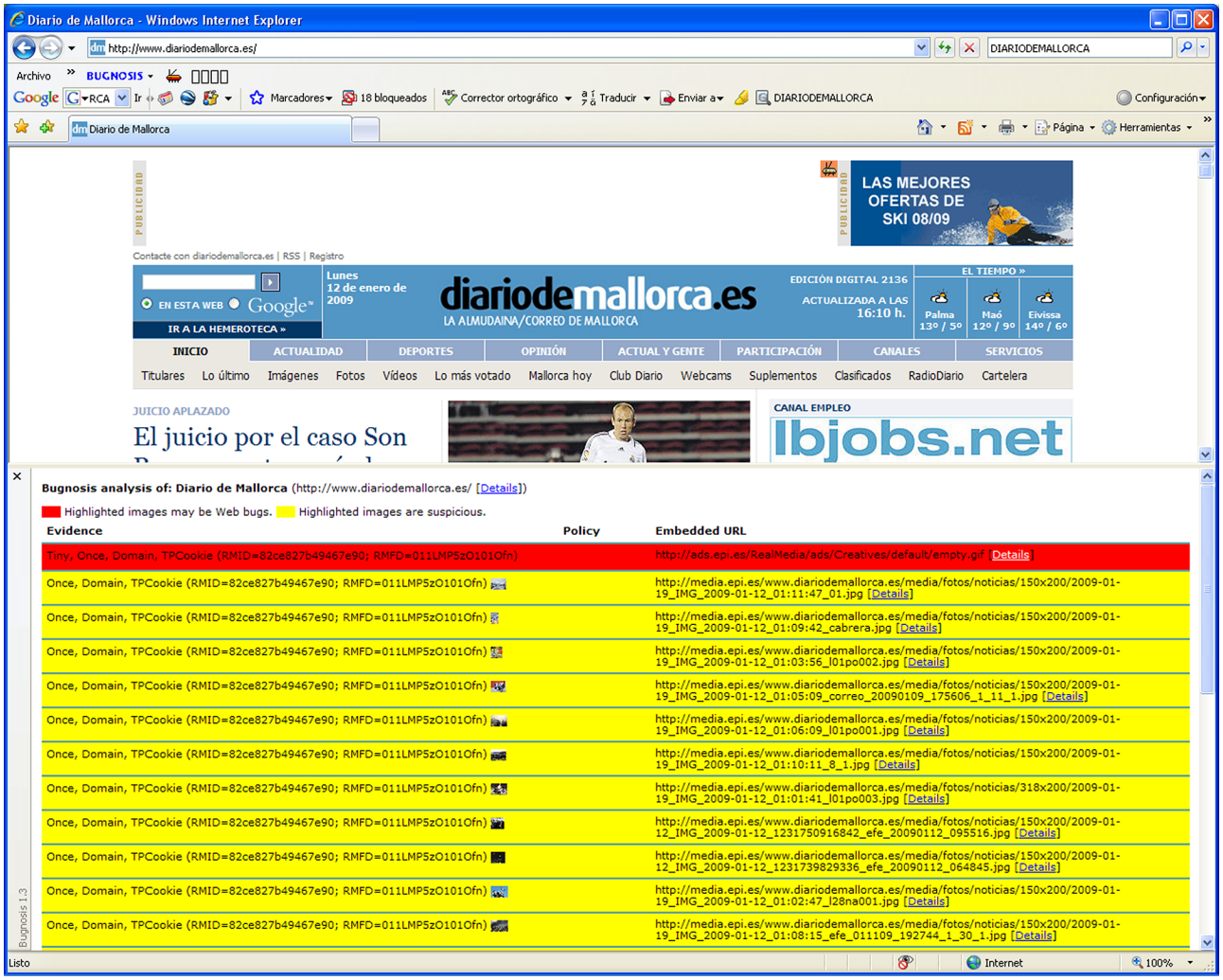
Los Servicios Premium a los que se puede acceder a través de la navegación móvil son actualmente Emoción y Pagos Movistar [...]. La introducción de los datos "x-up-subno" y "TM user-id" son necesarios para que Telefónica pueda facturar los servicios contratados por el cliente a través de estas plataformas [...]»

En este caso, queda probado que el enriquecimiento de cabeceras se dirigió a todos los usuarios y no solo a los usuarios de servicios Premium, sin que quedara probada la información previa y el consentimiento de acuerdo con el artículo 22.2 LSSICE. Por ello, la AEPD impuso a la entidad Telefónica Móviles España, S.A.U una multa de 20.000 euros por infracción del artículo 22.2 LSSICE.

Hay otros instrumentos de navegación que captan datos de los usuarios, entre ellos, los ***web bugs***. Son pequeñas imágenes incluidas en páginas web. La visualización de la imagen provoca la ejecución de una acción determinada. Los *web bugs* pasan desapercibidos (pueden ser imágenes de un píxel transparente) y pueden obtener información de los usuarios que se conectan a la página web en la cual han sido introducidos. También pueden estar vinculados a un archivo. ¿Qué hacen? Pueden recoger estadísticas de uso y visualización de pá-

ginas web, crear un perfil del usuario, transferir información de un sitio web a una empresa de marketing, controlar la efectividad de las barras publicitarias, etc. Pueden obtener la dirección IP, el navegador utilizado o la información contenida en las *cookies* (como ejemplo, un *web bug* puede leer el número de una *cookie* identificada y la información vuelve a la empresa que ha instalado el *web bug*).

Ejemplo:



Los ***mail bugs*** son imágenes de las mismas características que los *web bugs*, pero asociadas al correo electrónico. También pasan desapercibidos para el usuario. Cuando se visualice el mensaje, la imagen se descargará del servidor, revelará que el mensaje que lo contiene ha sido abierto y verifica la dirección de correo electrónico, con lo que habrá obtenido esta dirección que seguramente usará para el envío de comunicaciones comerciales no solicitadas.

Los **programas espía** o ***spyware*** instalan un determinado programa en el ordenador del afectado sin que este ni siquiera se dé cuenta y recogen información sin afectar a la integridad el sistema. Los datos de los usuarios pueden llegar a ser utilizados por terceros que nunca han tenido ningún tipo de rela-

ción con el usuario y este no es consciente de que tiene un archivo espía en su ordenador. A veces se instalan con programas gratuitos e incluso puede que estén en las condiciones de la instalación de estos programas. La información obtenida se utiliza con bastante frecuencia para generar publicidad específica para ese usuario, conocer la dirección de correo electrónico, los sitios que ha visitado, etc.

Los ***adware*** solo muestran publicidad mientras el usuario está utilizando una determinada aplicación. Durante la instalación, el *adware* entra en el ordenador (por ejemplo, con la instalación de un programa gratuito) y se auto ejecuta cada vez que se inicia una sesión, recoge las páginas que visita, lo envía a servidores externos que después enviarán publicidad al usuario.

Ante todos estos instrumentos de navegación, hay que plantearse cuestiones como cuáles son los datos recogidos, ya que habrá datos de carácter personal, la necesidad de consentimiento, la cesión de datos a terceros, así como las finalidades en la utilización de estos datos.

6.2. Normativa aplicable a las *cookies* y a otros instrumentos de almacenamiento de información

Si bien esta cuestión está en vías de ser modificada por la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas, debemos citar primero la Directiva sobre Privacidad y Comunicaciones Electrónicas, que en su considerando 25 establece que los instrumentos de almacenamiento de información pueden tener un uso legítimo y resultar de gran utilidad para, por ejemplo, analizar la efectividad del diseño y la publicidad de un sitio web o para verificar la identidad de los participantes en una transacción en línea. En el caso que tengan un propósito legítimo, debe autorizarse su uso e informar a los usuarios de forma clara y precisa para que sepan y sean conscientes de la información que se está introduciendo en su equipo, teniendo la posibilidad de oponerse a la instalación de esos dispositivos. En relación con la información que se ha de facilitar, establece este considerando 25 que:

> «La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato" (*cookie*) o dispositivo similar, en caso de que este tenga un propósito legítimo.»

En relación con esta cuestión y el considerando transcrito, el Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas (disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp126_es.pdf), del Grupo de Trabajo del Artículo 29, afirma:

«La última frase del considerando 25, "se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un 'chivato'", en caso de que este tenga un propósito legítimo, puede estar en contradicción con la afirmación de que los usuarios deben tener la posibilidad de impedir el almacenamiento de un "chivato" en sus ordenadores personales y por lo tanto puede requerir una aclaración o revisión.»

Todo ello se concreta en el artículo 5.3 de la Directiva:

«Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE, y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado.»

La regulación de las *cookies* en la normativa española se encuentra en el artículo 22.2 LSSICE, artículo que trae causa de lo establecido en la Directiva sobre Privacidad y Comunicaciones Electrónicas. Según este precepto:

- Los prestadores de servicios de la sociedad de la información podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios si:
  - Estos han dado su consentimiento.
  - Una vez que han recibido información clara y completa sobre su utilización.
  - Y, en particular, sobre los fines del tratamiento de acuerdo con lo establecido en la LOPDP.

- Cuando técnicamente sea posible y eficaz, este consentimiento podrá facilitarse mediante el uso de los parámetros del navegador o de otras aplicaciones.

- Ello no impide el almacenamiento o acceso a los datos con el único fin de efectuar una transmisión de una comunicación por una red de comunicaciones electrónicas o para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario. En relación con la exención de consentimiento se puede ver el «Dictamen 4/2012 sobre la exención del requisito de consentimiento de *cookies*» del Grupo de Trabajo del Artículo 29, adoptado el 7 de junio de 2012 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf).

Sobre el consentimiento en el uso de *cookies*, el «Working Document 02/2013 providing guidance on obtaining consent for cookies» del Grupo de Trabajo del Artículo 29, de 2 de octubre de 2013 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf), se refiere a los elementos necesarios para que pueda darse un consentimiento válido y los enumera así:

«The opinion on consent provides further clarity on the requirements of valid consent and its main elements:

1. Specific information. To be valid, consent must be specific and based on appropriate information. In other words, blanket consent without specifying the exact purpose of the processing is not acceptable.

2. Timing. As a general rule, consent has to be given before the processing starts.

3. Active choice. Consent must be unambiguous. Therefore the procedure to seek and to give consent must leave no doubt as to the data subject's intention. There are in principle no limits as to the form consent can take. However, for consent to be valid it should be an active indication of the user's wishes. The minimum expression of an indication could be any kind of signal, sufficiently clear to be capable of indicating a data subject's wishes, and to be understandable by the data controller (it could include a handwritten signature affixed at the bottom of a paper form, or an active behaviour from which consent can be reasonably concluded).

4. Freely given. Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.»

Sin embargo, esta regulación cambiará en breve con una nueva regulación contenida en la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas. El considerando 22 de esta Propuesta se dedica a esta cuestión, que después se concreta en el artículo 8.

La primera cuestión que destaca este proyecto normativo es el de la necesidad de utilizar métodos sencillos para la obtención del consentimiento del usuario final. Entiende que ahora los usuarios se encuentran agobiados por las solicitudes constantes de consentimiento. Como solución se plantea el uso de medios técnicos para dar el consentimiento a través de parámetros transparentes y sencillos. Entiende que una posibilidad es dar el consentimiento mediante los ajustes apropiados del navegador o de otra aplicación, que deberán ser vinculantes y oponibles a terceros.

Destaca el papel de los navegadores que intervienen en gran parte de lo que ocurre entre el usuario final y el sitio web, por lo que «ocupan una posición privilegiada para desempeñar un papel activo con el fin de ayudar a los usuarios finales a controlar el flujo de información que reciben y emiten los equipos terminales».

El considerando 23 afirma que los usuarios finales han de disponer de una serie de opciones en la configuración del navegador que vayan del nivel más elevado de protección («no aceptar nunca *cookies*») al nivel más bajo (aceptarlas siempre). Lo que hay que destacar de este considerando es que estos ajustes de privacidad han de presentarse de forma bien visible e inteligible. Además, en el considerando 24 establece que es conveniente que los navegadores

propongan a los usuarios finales métodos sencillos para modificar la configuración sobre la privacidad en cualquier momento y puedan excluir o aceptar determinados sitios web o especificar en qué sitios web aceptan siempre o no aceptan nunca *cookies* (de terceros).

Todo ello se concreta, como decíamos, en el artículo 8 de la Propuesta de Reglamento, que prohíbe con carácter general el uso de las capacidades de tratamiento y almacenamiento de los equipos terminales y la recopilación de información del equipo terminal de los usuarios finales, incluida la relativa a su soporte físico y lógico –excepto por parte del usuario final–, salvo:

- Cuando sean necesarios con el fin exclusivo de efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas.

- Cuando el usuario final haya dado su consentimiento.

- Cuando sean necesarios para la prestación de un servicio de la sociedad de la información solicitado por el usuario final.

- Cuando sean necesarios para medir la audiencia en la web, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final.

Por otra parte, según el artículo 8.2, se prohíbe recopilar la información emitida por un equipo terminal para poder conectarse a otro dispositivo o a un equipo de red, excepto en los siguientes casos:

- Cuando se lleva a cabo con el fin exclusivo de establecer una conexión y solamente durante el tiempo necesario para ello.

- Cuando se muestre una advertencia clara y destacada que informe, como mínimo, de las modalidades de recopilación, su finalidad, las personas responsables de ella y la información restante requerida de acuerdo con el Reglamento de protección de datos, cuando se recojan datos personales, así como de las medidas que puede adoptar el usuario final del equipo terminal para interrumpir o reducir al mínimo la recopilación.

Esta información se podrá proporcionar en combinación con el uso de iconos normalizados que ofrezcan, «de forma fácilmente visible, inteligible y claramente legible», una adecuada visión de conjunto.

Por otra parte, el artículo 10 de la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas se refiere a la información y las opciones de configuración de privacidad que deben ofrecerse al usuario. En este sentido, los programas informáticos ofrecerán la posibilidad de impedir a terceros almacenar información sobre el equipo terminal del usuario final o información

almacenada en el mismo. Al iniciarse la instalación del programa, se deberá informar al usuario de las opciones de configuración de confidencialidad y antes de continuar la instalación se solicitará el consentimiento en relación a una configuración determinada.

Volviendo a las normas antes mencionadas y vigentes a día de hoy sobre la materia, se requiere información clara y completa sobre su utilización y finalidad más la posibilidad de rechazar el tratamiento de datos mediante un procedimiento sencillo y gratuito de oposición. Después de lo expuesto en cuanto a la descripción de *web bugs*, *mail bugs* o *spyware*, difícilmente se cumplen los requisitos establecidos ni por la Directiva ni por la LSSICE en su artículo 22.2, lo que conlleva a su vez el incumplimiento de muchos de los requisitos que establecen las normas sobre protección de datos, para el uso de datos de carácter personal de forma lícita.

El ya mencionado «Working Document 02/2013 providing guidance on obtaining consent for cookies» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf), se refiere al modo de presentar la información requerida por la norma europea en materia de privacidad y comunicaciones comerciales para el uso de *cookies*. En este sentido, afirma que es necesario:

«- An immediately visible notice that various types of *cookies* are being used by the website, providing information in a layered approach, typically providing a link, or series of links, where the user can find out more about types of *cookies* being used.

- An immediately visible notice that by using the website, the user agrees to *cookies* being set by the websites,

- Information as to how the users can signify and later withdraw their wishes regarding *cookies* including information on the action required to express such a preference.

- A mechanism by which the user can choose to accept all or some or decline *cookies*.

- An option for the user to subsequently change a prior preference regarding *cookies*.»

Para la aplicación correcta de la normativa actual en relación con las *cookies*, la AEPD preparó una «Guía para el uso de *cookies*» (disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf). Esta guía establece la forma como debe presentarse la información y la solicitud de consentimiento para el uso de *cookies* de forma lícita. Se basa en una información por capas. La primera capa mostrará la siguiente información:

- Advertencia sobre el uso de *cookies* no exceptuadas por el artículo 22.2 LSSICE que se instalan al navegar por los sitios web o al utilizar el servicio solicitado. (Las excepciones son el almacenamiento o acceso a los datos con el único fin de efectuar una transmisión de una comunicación por una red de comunicaciones electrónicas, o para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.)

- Identificación de las finalidades de las *cookies* que se instalan, con información sobre si se trata de *cookies* propias o de terceros.

- Advertencia, en su caso, de que si se realiza una determinada acción se entenderá que el usuario acepta el uso de las *cookies*.

- Un enlace a la segunda capa informativa en la que se indica una información más detallada.

La segunda capa deberá profundizar más al respecto y deberá incluir:

- Tipo de *cookies* que utiliza la página web y su finalidad.

- Forma de desactivar o eliminar las *cookies* descritas y forma de revocación del consentimiento ya prestado.

- Identificación de quienes utilizan las *cookies*, incluidos los terceros con los que el editor haya contratado la prestación de un servicio que suponga el uso de *cookies*.

Lectura recomendada

Sobre esta cuestión, véase:
J. Aparicio Salom; S. Sanfulgencio Tomé (2014). «El régimen jurídico de las *cookies* y su aplicación por la Agencia Española de Protección de datos». *Revista Aranzadi Doctrinal* (núm. 11/2014. BIB 2014\675).

Los epígrafes 3 y 4 del artículo 31 del Código Ético de Confianza Online, en relación a las *cookies* y a otros instrumentos capaces de recabar información de los usuarios, establecen que:

> «3. Las *cookies* u otras técnicas se utilizarán de forma disociada y nunca individualizada o relacionada con los datos personales de los usuarios, de forma que la información que se obtenga no pueda asociarse a persona identificada o identificable, salvo que el consumidor haya dado su consentimiento. En particular, cuando se utilicen *cookies* o *pixels* transparentes u otras técnicas asimilables, se proporcionará a los usuarios información clara y comprensible sobre su objetivo y su utilización desvinculada de cualquier dato de carácter personal.
>
> 4. El tratamiento de las *cookies* es extrapolable por analogía a otras técnicas de monitorización de la conducta de los usuarios en su utilización de medios electrónicos de comunicación a distancia.»

Además de la regulación actual de las *cookies*, hay que tener en cuenta –como ya ha quedado establecido anteriormente– la Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas. Como afirma en sus considerandos, ahora ya hay otras técnicas capaces de rastrear los comportamientos en línea de los usuarios finales, por lo que es necesario una nueva norma sobre la cuestión. A modo de ejemplo, el considerando 15 de esta Propuesta de Reglamento afirma que:

> «A medida que la tecnología avanza, aumentan también los medios técnicos para la interceptación. Dichos medios pueden abarcar desde la instalación de equipos que recopilan datos de los equipos terminales de las zonas seleccionadas, como los denominados receptores de IMSI (identidad internacional de abonado móvil), hasta algunos programas y técnicas que, por ejemplo, efectúan un seguimiento subrepticio de los hábitos de navegación para crear perfiles de usuarios finales. Otros ejemplos de interceptación pueden ser la captura de datos de la carga útil o de datos de contenido de redes y encaminadores inalámbricos sin cifrar, entre ellos los hábitos de navegación, sin el consentimiento de los usuarios finales.»

Por otra parte, esta Propuesta de Reglamento también pretende cambiar la regulación actual de las *cookies*. Entiende que los métodos empleados para suministrar información y obtener consentimiento del usuario deben ser lo más sencillos posibles. La regulación actual hace que el usuario tenga que dar su consentimiento en numerosas ocasiones; la Propuesta de Reglamento establece que esto se puede resolver con el uso de medios técnicos para dar el consentimiento, a través de parámetros transparentes y sencillos. Establece la posibilidad de manifestar el consentimiento mediante el uso de los ajustes adecuados del navegador o de otra aplicación y que las opciones elegidas tienen que ser vinculantes y oponibles a terceros. Según su considerando 22, los navegadores intervienen en gran parte de lo que ocurre entre el usuario final y el sitio web: «Desde este punto de vista, ocupan una posición privilegiada para desempeñar un papel activo con el fin de ayudar a los usuarios finales a controlar el flujo de información que reciben y emiten los equipos terminales. Más concretamente, los navegadores pueden servir para montar la guardia, ayudando a los usuarios finales a impedir el acceso a la información de su equipo terminal (por ejemplo, un teléfono inteligente, una tableta o un ordenador) o el almacenamiento de la misma».

El «Dictamen 1/2009» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp159_en.pdf) se mostraba en desacuerdo con la configuración predeterminada del navegador como autorización previa. Según este documento, las configuraciones predeterminadas de navegador deberían ser «respetuosas de la "privacidad", pero no pueden ser un medio de hacerse con la autorización libre, específica e informada de los usuarios», como se exige en el artículo 2, letra h), de la Directiva sobre la protección de los datos.

Entre las resoluciones de la AEPD, podemos citar la resolución R/00357/2017, instruida frente a la entidad PACSOLUTOR, S.L.U., sobre un incumplimiento del artículo 22.2 LSSICE en relación a la información sobre *cookies* de la empresa mencionada:

«El citado artículo 22.2 de la LSSI extiende su alcance a todos los tipos de dispositivos de almacenamiento y recuperación de datos utilizados por los prestadores de servicios de la sociedad de la información en cualesquiera equipos terminales de los destinatarios de dichos servicios, lo que incluye no solo las *cookies*, que son archivos o ficheros de uso generalizado que permiten almacenar datos en dichos equipos con diferentes finalidades, sino también cualquier otra tecnología similar utilizada para almacenar información o acceder a información almacenada en el equipo terminal. No hay que olvidar que, en muchos casos, los usuarios que utilizan los servicios de Internet desconocen que el acceso a los mismos puede conllevar la instalación de ficheros o archivos en sus equipos terminales y que, al ser recuperados con la información almacenada en los mismos, permiten no solo mejorar la navegación y prestar correctamente el servicio solicitado, sino que también posibilitan, con las implicaciones para la privacidad de los usuarios que ello supone, la recogida actualizada y continuada de datos relacionados con sus equipos y perfiles de navegación, que posteriormente podrán ser utilizados por los responsables de los sitios web a los que se accede, o por los terceros, para analizar su comportamiento y para el envío de publicidad basada en el mismo o como medio para el desarrollo de otros productos y servicios concretos.

Por lo tanto, para garantizar la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados, que con mayor frecuencia recurren a Internet para la realización de sus actividades cotidianas, la regulación comunitaria

y nacional establece la obtención de un consentimiento informado con el fin de asegurar que estos puedan conocer del uso de sus datos y las finalidades para las que son utilizados.»

En el caso concreto, «en fecha de 28/11/2016 se verificó que la página web analizada descargaba DARD de terceros con finalidades de análisis de la actividad de la web, y publicitarias, y en cuanto a la información que ofrecían al acceder (aviso de primera capa) no se deducía el tipo de DARD, y su finalidad, al incluir expresiones como [....] mejorar la experiencia de navegación, así como ofrecer una información y servicios más personalizados [...]. Por tanto, no puede entenderse que la citada página web proporciona información suficiente al usuario para otorgar su consentimiento informado, para permitir el uso de DARD. La conducta descrita está tipificada como leve en el artículo 38.4.g) de la citada norma, que señala como tal g) "utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2"».

En la resolución del recurso de reposición RR/00220/2017:

«En el presente procedimiento se imputa a A.A.A. la comisión de una infracción del artículo 22.2 de la LSSI. El citado artículo 22.2 de la LSSI extiende su alcance a todos los tipos de dispositivos de almacenamiento y recuperación de datos utilizados por los prestadores de servicios de la sociedad de la información en cualesquiera equipos terminales de los destinatarios de dichos servicios, lo que incluye no solo las *cookies*, que son archivos o ficheros de uso generalizado que permiten almacenar datos en dichos equipos con diferentes finalidades, sino también cualquier otra tecnología similar utilizada para almacenar información o acceder a información almacenada en el equipo terminal.

No hay que olvidar que en muchos casos los usuarios que utilizan los servicios de Internet desconocen que el acceso a los mismos puede conllevar la instalación de ficheros o archivos en sus equipos terminales y que, al ser recuperados con la información almacenada en los mismos, permiten no solo mejorar la navegación y prestar correctamente el servicio solicitado, sino que también posibilitan, con las implicaciones para la privacidad de los usuarios que ello supone, la recogida actualizada y continuada de datos relacionados con sus equipos y perfiles de navegación, que posteriormente podrán ser utilizados por los responsables de los sitios web a los que se accede, o por los terceros, para analizar su comportamiento y para el envío de publicidad basada en el mismo o como medio para el desarrollo de otros productos y servicios concretos. Por lo tanto, para garantizar la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados, que con mayor frecuencia recurren a Internet para la realización de sus actividades cotidianas, la regulación comunitaria y nacional establece la obtención de un consentimiento informado con el fin de asegurar que estos puedan conocer del uso de sus datos y las finalidades para las que son utilizados. [...].

En el presente supuesto, [...] el sitio web denunciado no ofrecía información respecto de la instalación de dispositivos de almacenamiento y recuperación de datos que cumpliera con el mandato del art. 22.2 de la LSSI. El modo de ofrecer la información del citado artículo no obedece a supuestos tasados, lo relevante es que cualquier fórmula que satisfaga la finalidad del precepto es perfectamente válida. Y si bien como sostiene la denunciada, las recomendaciones de la AEPD –Guía de *Cookies*– no tienen naturaleza de norma, es este organismo a quién le compete velar por el cumplimiento de la obligación de informar a fin de que los usuarios otorguen su consentimiento en óptimas condiciones y por tanto la interpretación del artículo, es decir, que exista información clara y completa, por lo que cualquier información no es suficiente, sino que deberá estar estrechamente vinculada con el tipo de DARD que se descarguen en los terminales de los usuarios. En este sentido debe recordarse que la "Guía sobre el uso de *cookies*", ofrece indicaciones al respecto, proponiendo un sistema de información por capas. De modo que la segunda capa complemente a la primera. En la primera capa debe mostrarse la información esencial sobre la existencia de *cookies*, si son propias o de terceros y las finalidades de las *cookies* empleadas, así como los modos de prestar el consentimiento. En cuanto a la información ofrecida en la segunda capa, esta Agencia ha venido indicando, singularmente en la Guía sobre el uso de *cookies*, que dicha información adicional y complementaria de la primera, debería versar sobre qué son y para qué se utilizan las *cookies*, los tipos de *cookies* utilizadas y su finalidad, así como la forma de desactivar o eliminar las *cookies* enunciadas a través de las funcionalidades facilitadas por el editor, las herramientas proporcionadas por el navegador o el terminal o a través de las plataformas comunes que pudieran existir, para esta finalidad o en su caso, la forma de revocación del consentimiento ya prestado. Finalmente, debe en esta segunda capa ofrecerse información sobre la identificación de quien utiliza las *cookies*, esto es, si la información obtenida por las

cookies es tratada solo por el editor y/o también por terceros. Con la identificación de aquellos con los que haya contratado o cuyos servicios ha decidido integrar el editor.

Por tanto, el suministro de la información adicional en una segunda capa por grupos de *cookies*, da cumplimiento al precepto, siempre que exista identidad entre ellas y ello no produzca ambigüedad, y en todo caso se indique si son de primera o de tercera parte, con identificación del tercero, y su finalidad, así como con alusión a los mecanismos de rechazo de las *cookies* enunciadas y la forma de revocación del consentimiento ya prestado. La normativa estudiada pretende que el usuario sea suficientemente informado sobre la utilización de dispositivos de almacenamiento y recuperación de datos en su equipo terminal, siendo esencial que dicha información verse sobre las finalidades de dichos dispositivos, pero sin exigir que la información detalle los nombres de todas y cada una de las *cookies* no exentas descargadas. Ahora bien, nada obsta a que dicha información adicional se ofrezca, a los efectos de dar cumplimiento a los requisitos de la segunda capa, en un cuadro adjunto que señale el dominio bajo el cual figura la *cookie*, su finalidad concreta, y si es propia o de tercera parte, con identificación, en su caso, del tercero en cuestión.

Es decir, aunque dicho sistema no sea exigible, la Agencia entiende que la descripción contenida en el citado cuadro puede dar cumplimiento a los requisitos de la segunda capa relativos a los tipos de *cookies* utilizadas y su finalidad, así como sobre quién utiliza las *cookies*, en la medida en que contenga la información exigible antes específica.»

En la resolución AEPD R/01753/2016 en el procedimiento sancionador PS/00005/2016 instruido por la Agencia Española de Protección de Datos a la entidad TELEFONICA MOVILES ESPAÑA, S.A.U., ya citada anteriormente, se trata de la utilización de la técnica de «enriquecimiento por cabeceras» por parte de Telefónica, técnica que se explica a continuación, siendo de aplicación al caso el artículo 22.2 LSSICE:

«UNO.- En el sitio web http://comunidad.movistar.es.....TME, ante una consulta de un usuario, reconoce que utiliza la técnica de "enriquecimiento de cabeceras".

DOS.- TME, en el escrito de fecha de entrada en esta Agencia de 01/12/2015, manifiesta lo siguiente:

"[...] El enriquecimiento de cabeceras es una funcionalidad utilizada únicamente en el protocolo HTTP que permite añadir meta-información a las peticiones de acceso a una página web concreta que se progresa desde el terminal del cliente hasta el servidor final [...] [...] en este contexto histórico, todos los terminales usaban proxy explícito para la navegación por el APN telefónica.es, ya que la navegación a través de la red móvil estaba más limitada que actualmente [...].

[...] a partir de 2012 se inicia un proceso de consolidación de la solución de Proxy de Navegación Móvil estando disponible para cualquier terminal que disponga de la configuración del APN telefónica.es. [...] en este proceso de consolidación se mantuvo por defecto la identificación de navegación ("x-up-subno" y "TM_user_ID") desde la red para sostener el modelo de negocio de contenidos Premium. [...]

[...] en septiembre de 2015 [...] se ha hecho un esfuerzo de racionalización de uso del enriquecimiento de cabeceras en la navegación móvil [...]"

TRES.- En fecha de 13/10/2015, se accede desde dos teléfonos móviles con contratos con Movistar a la página en Internet http://amibeingtracked.com/ con la finalidad de verificar si el operador utiliza "*supercookies*" en páginas que no son relativas a servicios Premium o que reclaman alguna facturación, siendo el resultado negativo.»

Y sigue afirmando la resolución que:

«[…] sitúa bajo su régimen sancionador a los Prestadores de Servicios de la Sociedad de la Información, entre los que se encuentran los prestadores de servicios de intermediación. Aunque fuera un servicio de intermediación, el presente caso no afecta a las previsiones del art. 14 de LSSI, sino al cumplimiento de las garantías recogidas en el art. 22.2 LSSI exigibles a todos los prestadores de servicios de la Sociedad de la Información incluidos los servicios de intermediación. En segundo lugar, debe señalarse que la utilización de la técnica de enriquecimiento de cabeceras se venía utilizando por TME, con independencia de su utilización para la finalidad que en principio estaba prevista, la facturación de los servicios Premium, ya que se utilizaba indistintamente para todos los usuarios. Por tanto, no siempre se podían considerar dispositivos de carácter técnico para los que la norma prevé la dispensa de la información

al usuario de acuerdo con el último párrafo del art. 22.2 LSSI, o dicho de otro modo, para aquellos usuarios que no utilizaran los servicios Premium, no era de aplicación la exención que prevé la norma y por tanto se hacía necesario el cumplimiento del deber de información. A esta conclusión – de utilización de dicha técnica de modo generalizado –se llega, precisamente, por las propias manifestaciones de TME durante las actuaciones previas de inspección, en concreto, en el escrito de fecha de entrada en esta Agencia de 01/12/2015 se hace constar lo siguiente: [...] El enriquecimiento de cabeceras es una funcionalidad utilizada únicamente en el protocolo http que permite añadir meta-información a las peticiones de acceso a una página web concreta que se progresan desde el terminal del cliente hasta el servidor final [...] [...] en este contexto histórico, todos los terminales usaban proxy explícito para la navegación por el APN telefónica.es ya que la navegación a través de la red móvil estaba más limitada que actualmente [...] [...] a partir de 2012 se inicia un proceso de consolidación de la solución de Proxy de Navegación Móvil estando disponible para cualquier terminal que disponga de la configuración del APN telefónica.es. [...] en este proceso de consolidación se mantuvo por defecto la identificación de navegación ("x-up-subno" y "TM_user_ID") desde la red para sostener el modelo de negocio de contenidos Premium. [...] (...) en septiembre de 2015 [...] se ha hecho un esfuerzo de racionalización de uso del enriquecimiento de cabeceras en la navegación móvil [...] Debe señalarse que el protocolo HTTP es el lenguaje que utiliza la comunicación entre el usuario/cliente y el servidor web. Es decir, facilita la comunicación que utilizan los distintos softwares web –tanto clientes, como servidores y proxis– para interactuar entre sí. Por tanto se puede afirmar que es utilizado por la generalidad de usuarios de internet para su navegación. Por lo que el adjetivo utilizado por TME en su explicación, –únicamente– tal vez no sea el más adecuado dado lo común en su utilización y que tiene como finalidad aminorar las consecuencias derivadas de la utilización de dicha técnica. En conclusión, se ha estado utilizando, en multitud de accesos y navegación en internet, la citada técnica hasta septiembre del año 2015.»

6.3. Análisis de algunos casos en España y en otros países

España: resolución AEPD 442/2004

En la resolución AEPD 442/2004, la persona que denuncia afirma: «Las empresas denunciadas me están agrediendo y afectando mi intimidad al inundar de "bichos" mi ordenador y no dejarme trabajar en paz, ya que mediante engaños instalé un certificado y ahora no puedo acceder a Internet sin sufrir molestias de inundación de páginas web no deseadas ni deseables». Se trataba de programas *adware* que se instalaban al realizar alguna conexión a Internet. Entre las condiciones de uso constaba: «El usuario acepta que se pueda instalar software gratuito para el usuario a cambio de anuncios publicitarios. Estos anuncios en los que se basa la gratuidad del software podrán ser mostrados en su ordenador en cualquier tiempo o periodo de tiempo». En este caso, se archivaron las actuaciones.

España: resolución AEDP 229/2006

En la resolución AEDP 229/2006 se trataba de entidades responsables de la instalación de productos software: EE.UU. y Canadá. Entre la información que recogían estaba la dirección IP del usuario, el tipo de navegador, el dominio, el sistema operativo, el idioma, el proveedor de servicios de Internet que gestiona la conexión, la información sobre las páginas visitadas, el software instalado en el equipo, el código postal.

EE. UU.: *cookies* y el caso Doubleclick

Se produjo una gran polémica cuando la empresa Doubleclick decidió asociar la información obtenida con las *cookies* a una gran base de datos que contenía millones de domicilios americanos. La empresa tuvo que dar una dirección donde los usuarios pudieran darse de baja.

EE. UU.: *adware* y *spyware*. Entre otras demandas: Enigma vs. Lavasoft

En Michigan se iniciaron procesos contra Doubleclick ya que esta compañía había violado las leyes relativas a la protección de los consumidores por no avisarles de que introducía regularmente *cookies* y *web bugs* en sus ordenadores. Gracias a ellos, Doubleclick fue capaz de identificar las preferencias sobre cruceros de más de diez millones de personas y les enviaba publicidad a medida, según sus gustos. Esta era su política de privacidad:

> «El sitio web de DoubleClick.com puede utilizar *cookies* persistentes, *web beacons* y los datos en nuestros registros (como su dirección de protocolo de Internet, la dirección del sitio web anterior, etc.) sobre su actividad en este sitio web para entender mejor cómo utiliza el sitio web, para resolver problemas técnicos y mejorar su experiencia. Los datos sobre su uso del sitio web no se cruzan con los datos de cualquier otra *cookie* de DoubleClick. Tampoco se combinan los datos de la *cookie* persistente sobre el análisis del sitio web con los datos incluidos en nuestros registros. Si nos facilita su dirección de correo electrónico en este sitio web, posiblemente se vincule esta *cookie* de análisis del sitio web a su dirección de correo electrónico para enviarle correo electrónico sobre los productos y servicios de DoubleClick [...].»

Right Media también utiliza *cookies*, *web beacons* o *clearpixels* y archivos log. Esta empresa declara que estas técnicas se usan para recopilar datos no identificables, aunque entre ellos está la dirección IP del usuario.

EE. UU.: caso Zango

La Federal Trade Comission propuso un acuerdo a la empresa Zango, que utilizaba *spyware* y *adware* para el tratamiento de información, que:

- Le prohibía instalar cualquier programa, código o contenido en los ordenadores de los consumidores sin su consentimiento expreso.
- Le obligaba a informar al consumidor previamente de manera clara, destacada y separada.
- Le obligaba a ofrecer al consumidor los medios para desinstalar la aplicación.

EE. UU.: propuestas de ley federal

Estas propuestas, más específicas, requieren un «consentimiento específico del usuario» en base a preguntas como:

- «Este programa recogerá y transmitirá información acerca de usted. ¿Lo acepta?»

- «Este programa recogerá información acerca de los sitios web que visite y utilizará esta información para mostrar publicidad en su ordenador. ¿Lo acepta?»

6.4. La creación de perfiles a partir de los datos del usuario

El uso de *cookies* permite, en muchas ocasiones, la elaboración de perfiles de los usuarios, lo que posibilita enviar publicidad mucho más personalizada. A ello ya se refería el «Dictamen 2/2010 sobre publicidad comportamental en línea» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf) en estos términos:

> «Los proveedores de redes de publicidad y los editores deben proporcionar información a los usuarios en cumplimiento del artículo 10 de la Directiva 95/46/CE. En la práctica, deben garantizar que se comunique a los usuarios, como mínimo, quién (es decir, qué entidad) es responsable de instalar el *cookie* y recoger la información anexa. Además, los usuarios deben estar informados de manera sencilla de: a) que el *cookie* se utiliza para construir perfiles; b) qué tipo de información se recogerá para construir dichos perfiles; c) que los perfiles se utilizan para suministrar publicidad a medida del usuario y d) que el *cookie* permite identificar al usuario en múltiples sitios web.»

El RGPD, en su artículo 4, define la **elaboración de perfiles** como «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física». Al tratarse de un tratamiento de datos de carácter personal, tendrá que cumplirse todo lo establecido en el RGPD para que sea lícito.

Y en su artículo 22 sobre decisiones individuales automatizadas, incluida la elaboración de perfiles, afirma que todo interesado tendrá derecho a no ser objeto de una decisión basada en la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, a menos que la decisión:

> «a) Sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
>
> b) Esté autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
>
> c) Se base en el consentimiento explícito del interesado.»

En los casos de las letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos, las libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

7. Información precontractual y protección del consumidor

El deber de información es un deber básico y un pilar sobre el que se basa toda la normativa sobre protección del consumidor y, como se ha visto, también lo es en el ámbito de la protección de datos, donde es fundamental, con carácter general, el consentimiento prestado después de recibir información de manera clara, comprensible y adecuada al destinatario (por ejemplo, en el caso de menores, tiene que adecuarse a ellos, como se analizará en el apartado siguiente). Coinciden, con carácter general, los requisitos de forma de esta información, tanto para dar el consentimiento para el tratamiento de datos personales, como para celebrar un determinado contrato sobre bienes o servicios, cambiando el contenido de la información que se debe proporcionar en un caso y en otro.

Al deber de información y al principio de transparencia dedica el Reglamento General de Protección de Datos el artículo 12:

> «El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.»

Es entonces necesario que el responsable del tratamiento facilite información:

- en forma concisa, transparente, inteligible y de fácil acceso,
- en un lenguaje claro y sencillo (especialmente, la información dirigida a los niños).

Esta información será facilitada por escrito o por otros medios, incluidos los medios electrónicos. El contenido de esta información se enumera en los artículos 13 y 14, distinguiendo la información que ha de facilitarse cuando los datos se obtengan del interesado y cuando estos datos no se hayan obtenido del interesado. A modo de ejemplo, el artículo 13.2.f) establece que el responsable del tratamiento facilitará al usuario la información necesaria para garantizar un tratamiento de datos leal y transparente sobre la existencia de decisiones automatizadas, incluida la elaboración de perfiles, e información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. El artículo 14.4, por su parte, señala que cuando el responsable del tratamiento proyecte el tratamiento ulterior dedicado a otros fines, deberá informar al interesado sobre estos otros fines.

En relación a la información y transparencia a la que hacen referencia los artículos 13 y 14 del RGPD, el Anteproyecto de Ley de Protección de Datos de Carácter Personal establece en su artículo 21 que:

> «1. La información al afectado a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 deberá ser clara y concisa, así como fácilmente accesible y comprensible por el destinatario de la misma.
>
> Cuando la información vaya dirigida a menores de edad deberá además estar adaptada a esta circunstancia.
>
> 2. Cuando los datos de carácter personal sean obtenidos del afectado a través de redes de comunicaciones electrónicas o en el marco de la prestación de un servicio de la sociedad de la información, así como en aquellos otros supuestos expresamente establecidos por la ley o cuando así lo autorice la Agencia Española de Protección de Datos, el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica para acceder fácilmente a la restante información.
>
> 3. La información básica a la que se refiere el apartado anterior deberá contener al menos:
>
> a) La identidad del responsable del tratamiento o de su representante, en su caso.
>
> b) La finalidad del tratamiento.
>
> c) El modo en que el afectado podrá ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
>
> Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que pudieran producir efectos jurídicos sobre él o afectarle significativamente.
>
> 4. Cuando los datos de carácter personal no hubieran sido obtenidos del afectado el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquél la información básica señalada en el apartado anterior, indicándole una dirección electrónica para acceder fácilmente a la restante información.
>
> En estos supuestos, la información básica incluirá también:
>
> a) Las categorías de datos objeto de tratamiento.
>
> b) Las fuentes de la que procedieran los datos.»

Tanto desde el punto de vista de la contratación como de la protección de datos, es fundamental la información previa al consentimiento, la correspondiente en cada caso. Hay que distinguir la información previa del producto o servicio contratado, información que exigen todas las normas que afectan a la contratación y que tiene su repercusión en el ámbito contractual, de la información en relación al tratamiento de datos de carácter personal en, por ejemplo, el uso de *cookies* o en la elaboración de perfiles.

Centrándonos en el ámbito de la **contratación**, es muy importante la información previa sobre el producto o servicio, sobre el proveedor, las garantías, etc., que se exige en todas las normas: TRLGDCU, en general, y en sede de contratos a distancia y otros en particular, la LSSICE y la normativa sectorial correspondiente según el producto o servicio objeto del contrato.

Con carácter general, el artículo 20 TRLGDCU se refiere a la información necesaria en la oferta comercial de bienes y servicios:

«1. Las prácticas comerciales que, de un modo adecuado al medio de comunicación utilizado, incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, deberán contener, si no se desprende ya claramente del contexto, al menos la siguiente información:

a) Nombre, razón social y domicilio completo del empresario responsable de la oferta comercial y, en su caso, nombre, razón social y dirección completa del empresario por cuya cuenta actúa.

b) Las características esenciales del bien o servicio de una forma adecuada a su naturaleza y al medio de comunicación utilizado.

c) El precio final completo, incluidos los impuestos, desglosando, en su caso, el importe de los incrementos o descuentos que sean de aplicación a la oferta y los gastos adicionales que se repercutan al consumidor o usuario.

En el resto de los casos en que, debido a la naturaleza del bien o servicio, no pueda fijarse con exactitud el precio en la oferta comercial, deberá informarse sobre la base de cálculo que permita al consumidor o usuario comprobar el precio. Igualmente, cuando los gastos adicionales que se repercutan al consumidor o usuario no puedan ser calculados de antemano por razones objetivas, debe informarse del hecho de que existen dichos gastos adicionales y, si se conoce, su importe estimado.

d) Los procedimientos de pago, plazos de entrega y la ejecución del contrato y el sistema de tratamiento de las reclamaciones, cuando se aparten de las exigencias de la diligencia profesional, entendiendo por tal la definida en el artículo 4.1 de la Ley de Competencia Desleal.

e) En su caso, existencia del derecho de desistimiento.

2. El incumplimiento de lo dispuesto en el apartado anterior será considerado práctica desleal por engañosa en iguales términos a los que establece el artículo 7 de la Ley 3/1991, de 10 de enero, de Competencia Desleal.»

En sede de contratación, los artículos 60, 61 y 62 TRLGDCU se refieren a la información previa que el empresario debe facilitar antes de perfeccionarse cualquier contrato, incluyendo los artículos 60 bis y 60 ter sobre los pagos adicionales y los cargos por la utilización de determinados medios de pago, artículos necesarios ante algunas técnicas comerciales que se habían ido asentando en la contratación electrónica de determinados productos o servicios:

«**Artículo 60. Información previa al contrato**

1. Antes de que el consumidor y usuario quede vinculado por un contrato u oferta correspondiente, el empresario deberá facilitarle de forma clara y comprensible, salvo que resulte manifiesta por el contexto, la información relevante, veraz y suficiente sobre las características principales del contrato, en particular sobre sus condiciones jurídicas y económicas.

2. Serán relevantes las obligaciones de información sobre los bienes o servicios establecidas en esta norma y cualesquiera otras que resulten de aplicación y, además:

a) Las características principales de los bienes o servicios, en la medida adecuada al soporte utilizado y a los bienes o servicios.

b) La identidad del empresario, incluidos los datos correspondientes a la razón social, el nombre comercial, su dirección completa y su número de teléfono y, en su caso, del empresario por cuya cuenta actúe.

c) El precio total, incluidos todos los impuestos y tasas. Si por la naturaleza de los bienes o servicios el precio no puede calcularse razonablemente de antemano o está sujeto a la elaboración de un presupuesto, la forma en que se determina el precio así como todos

los gastos adicionales de transporte, entrega o postales o, si dichos gastos no pueden ser calculados razonablemente de antemano, el hecho de que puede ser necesario abonar dichos gastos adicionales.

En toda información al consumidor y usuario sobre el precio de los bienes o servicios, incluida la publicidad, se informará del precio total, desglosando, en su caso, el importe de los incrementos o descuentos que sean de aplicación, de los gastos que se repercutan al consumidor y usuario y de los gastos adicionales por servicios accesorios, financiación, utilización de distintos medios de pago u otras condiciones de pago similares.

d) Los procedimientos de pago, entrega y ejecución, la fecha en que el empresario se compromete a entregar los bienes o a ejecutar la prestación del servicio.

e) Además del recordatorio de la existencia de una garantía legal de conformidad para los bienes, la existencia y las condiciones de los servicios posventa y las garantías comerciales.

f) La duración del contrato, o, si el contrato es de duración indeterminada o se prolonga de forma automática, las condiciones de resolución. Además, de manera expresa, deberá indicarse la existencia de compromisos de permanencia o vinculación de uso exclusivo de los servicios de un determinado prestador así como las penalizaciones en caso de baja en la prestación del servicio.

g) La lengua o lenguas en las que podrá formalizarse el contrato, cuando no sea aquella en la que se le ha ofrecido la información previa a la contratación.

h) La existencia del derecho de desistimiento que pueda corresponder al consumidor y usuario, el plazo y la forma de ejercitarlo.

i) La funcionalidad de los contenidos digitales, incluidas las medidas técnicas de protección aplicables, como son, entre otras, la protección a través de la gestión de los derechos digitales o la codificación regional.

j) Toda interoperabilidad relevante del contenido digital con los aparatos y programas conocidos por el empresario o que quepa esperar razonablemente que conozca, como son, entre otros, el sistema operativo, la versión necesaria o determinados elementos de los soportes físicos.

k) El procedimiento para atender las reclamaciones de los consumidores y usuarios, así como, en su caso, la información sobre el sistema extrajudicial de resolución de conflictos prevista en el artículo 21.4.

3. El apartado 1 se aplicará también a los contratos para el suministro de agua, gas o electricidad –cuando no estén envasados para la venta en un volumen delimitado o en cantidades determinadas–, calefacción mediante sistemas urbanos y contenido digital que no se preste en un soporte material.

4. La información precontractual debe facilitarse al consumidor y usuario de forma gratuita y al menos en castellano.

Artículo 60 bis. Pagos adicionales

1. Antes de que el consumidor y usuario quede vinculado por cualquier contrato u oferta, el empresario deberá obtener su consentimiento expreso para todo pago adicional a la remuneración acordada para la obligación contractual principal del empresario. Estos suplementos opcionales se comunicarán de una manera clara y comprensible y su aceptación por el consumidor y usuario se realizará sobre una base de opción de inclusión. Si el empresario no ha obtenido el consentimiento expreso del consumidor y usuario, pero lo ha deducido utilizando opciones por defecto que este debe rechazar para evitar el pago adicional, el consumidor y usuario tendrá derecho al reembolso de dicho pago.

2. Corresponde al empresario probar el cumplimiento de las obligaciones a que este artículo se refiere.

Artículo 60 ter. Cargos por la utilización de medios de pago

1. Los empresarios no podrán facturar a los consumidores y usuarios, por el uso de determinados medios de pago, cargos que superen el coste soportado por el empresario por el uso de tales medios.

2. Corresponde al empresario probar el cumplimiento de las obligaciones a que este artículo se refiere.»

No hay que olvidar toda la información y aceptación de las condiciones generales de la contratación, también reguladas en el TRLGDCU. Con posterioridad a la celebración del contrato, la Ley exige una confirmación documental de la información proporcionada (artículo 63 TRLGDCU). Los artículos 97 y siguientes TRLGDCU establecen los deberes de información específica para los casos de contratación a distancia, que incluyen tanto los deberes previos de información como la documentación posterior al contrato. Y cuando se trata de contratos celebrados por vía electrónica, se aplicará además la LSSICE. Su artículo 10 se refiere a la información precontractual y el artículo 28, a los deberes posteriores a la contratación, con la obligación de enviar un acuse de recibo.

Según el artículo 10 LSSICE, previamente a la celebración del contrato, hay que informar de:

«1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga

de programas informáticos que efectúen funciones de marcación deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a) Las características del servicio que se va a proporcionar.

b) Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.

c) El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y

d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.»

Y los deberes posteriores a la contratación se regulan en el artículo 28 LSSICE:

«**Artículo 28. Información posterior a la celebración del contrato**

1. El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios:

a) El envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación, o

b) La confirmación, por un medio equivalente al utilizado en el procedimiento de contratación, de la aceptación recibida, tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario.

En los casos en que la obligación de confirmación corresponda a un destinatario de servicios, el prestador facilitará el cumplimiento de dicha obligación, poniendo a disposición del destinatario alguno de los medios indicados en este apartado. Esta obligación será exigible tanto si la confirmación debiera dirigirse al propio prestador o a otro destinatario.

2. Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello.

En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia desde que aquel haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

3. No será necesario confirmar la recepción de la aceptación de una oferta cuando:

a) Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o

b) El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación.»

También es importante distinguir la publicidad de la oferta, así como la regla que establece el artículo 61 sobre la integridad de la publicidad, promoción u oferta en el contrato:

«El contenido de la oferta, promoción o publicidad, las prestaciones propias de cada bien o servicio, las condiciones jurídicas o económicas y garantías ofrecidas serán exigibles por los consumidores y usuarios, aun cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido y deberán tenerse en cuenta en la determinación del principio de conformidad con el contrato.»

Solo en el caso de que el contrato contuviera cláusulas más beneficiosas para el consumidor, estas prevalecerán sobre la oferta, promoción y publicidad.

Como ejemplo que diferencia la publicidad de la oferta contractual, puede ser ilustrativo el considerando 12 de la Directiva (UE) 2015/2302 (disponible en: https://www.boe.es/doue/2015/326/L00001-00033.pdf), del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, relativa a los viajes combinados y a los servicios de viaje vinculados, por la que se modifican el Reglamento (CE), nº 2006/2004 y la Directiva 2011/83/UE del Parlamento Europeo y del Consejo y por la que se deroga la Directiva 90/314/CEE del Consejo:

« [...] Los servicios de viaje vinculados en línea deben distinguirse asimismo de sitios web a los que se accede mediante un enlace cuya finalidad no es la celebración de un contrato con el viajero, y de los enlaces a través de los cuales simplemente se informa a los viajeros sobre otros servicios de viaje de modo general, por ejemplo cuando un hotel o el organizador de un acontecimiento incluye en su sitio web una lista de todos los empresarios que ofrecen servicios de transporte a su establecimiento con independencia de cualquier reserva, o si se utilizan "*cookies*" o metadatos para insertar publicidad en sitios web.»

Pensemos en algún ejemplo que compagine ambas situaciones. Puede ser el caso de la instalación de un software, por ejemplo, un *spyware*, con lo que se estarían vulnerando los derechos de los usuarios por instalar un programa en el ordenador sin haber informado previamente, faltando la aceptación del consumidor y, además, por no haber informado ni obtenido el consentimiento para el tratamiento de sus datos de carácter personal.

Además, para la celebración del contrato será necesario obtener datos personales del consumidor, que estarían dentro de los datos necesarios para la celebración del contrato por lo que se refiere a las normas sobre protección de datos de carácter personal.

Lectura recomendada

El «Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online», realizado por la AEPD y el Instituto Nacional de Tecnologías de la Información (INTECO) en el año 2009, se refiere también a los derechos de los onsumidores en este ámbito, un tema que puede ser interesante en relación a este punto.

Agencia Española de Protección de Datos; Instituto Nacional de Tecnologías de la Información (2009). «Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online». Madrid: Instituto Nacional de Tecnologías de la Comunicación. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.

8. Publicidad, protección de datos y menores

Las referencias a los menores de edad en las normas sobre publicidad y también en otras van siendo cada vez más frecuentes. El artículo 3.b) de la Ley 34/1988, de 11 de noviembre –modificada por la Ley 29/2009, de 30 de diciembre–, considera que es ilícita:

> «La publicidad dirigida a menores que les incite a la compra de un bien o de un servicio, explotando su inexperiencia o credulidad, o en la que aparezcan persuadiendo de la compra a padres o tutores. No se podrá, sin un motivo justificado, presentar a los niños en situaciones peligrosas. No se deberá inducir a error sobre las características de los productos, ni sobre su seguridad, ni tampoco sobre la capacidad y las aptitudes necesarias en el niño para utilizarlos sin producir daño para sí o a terceros.»

Y en el caso de la información, el artículo 12 del Reglamento General de Protección de Datos, relativo al principio de transparencia, señala que «la información será de fácil acceso, con un lenguaje claro y sencillo, especialmente cuando esta información va dirigida a los niños».

La Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, modificada por la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y la adolescencia, establece el derecho de los menores a buscar, recibir y utilizar información adecuada a su desarrollo, haciendo especial mención a la alfabetización digital y mediática, de forma adecuada a cada etapa evolutiva. Y afirma que las Administraciones Públicas «velarán porque los medios de comunicación en sus mensajes dirigidos a menores promuevan los valores de igualdad, solidaridad, diversidad y respeto a los demás, eviten imágenes de violencia, [...]». De acuerdo con el RGPD, hay que tener especialmente en cuenta la privacidad desde el diseño cuando los principales destinatarios sean menores. Por otra parte, no hay que olvidar que las normas que modifican el sistema de protección de la infancia y la adolescencia de 2015 abogan por el grado de madurez del menor en lugar del criterio de la edad.

El «Dictamen 2/2010 sobre publicidad comportamental en línea» del Grupo de Trabajo del artículo 29 (disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_es.pdf) también se refería a la protección de los datos personales de los niños, afirmando que los problemas relativos a la obtención del consentimiento de los niños merecen especial atención. Como ya hemos comentado, en muchos casos hará falta el consentimiento de los representantes legales. Respecto al caso de la publicidad comportamental, afirma que:

> «En el caso que nos ocupa, esto supone que los proveedores de redes de publicidad podrían tener que informar a los padres de la recogida y utilización de datos del niño y obtener su consentimiento antes de recoger dichos datos y seguir utilizando la información con fines de realizar publicidad a medida para niños.»

Y añade otra cuestión importante:

> «En vista de lo que precede y teniendo también en cuenta la vulnerabilidad de los niños, el Grupo de Trabajo del Artículo 29 estima que los proveedores de redes de publicidad no deben ofrecer grupos de interés dirigidos a enviar publicidad comportamental a los niños o influir en ellos.»

La preocupación por la protección de datos de los menores es una constante en los informes y dictámenes del Grupo de Trabajo del Artículo 29. Así, en su «Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes» (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf) se afirma:

> «Los niños son ávidos usuarios de aplicaciones, ya sea en dispositivos propios o en dispositivos compartidos (con sus padres, sus hermanos o en un centro educativo), y existe claramente un gran mercado de aplicaciones diversas destinadas a ellos. Pero, al mismo tiempo, los niños apenas comprenden o conocen, si es que lo hacen en absoluto, el alcance y la sensibilidad de los datos a los que las aplicaciones pueden acceder, o el alcance de los datos compartidos con terceros para fines publicitarios.
>
> Los desarrolladores de aplicaciones y otros responsables del tratamiento de datos deben prestar atención al límite de edad que define a los niños y los menores de edad en las legislaciones nacionales, donde el consentimiento parental al tratamiento de datos es una condición previa para que las aplicaciones traten datos de forma lícita.
>
> Cuando el consentimiento puedan darlo legalmente los menores y la aplicación esté destinada a niños o menores, el responsable del tratamiento de datos debe prestar atención a las posibles limitaciones de comprensión y atención de los menores sobre dicho tratamiento.
>
> Debido a su vulnerabilidad general, y teniendo en cuenta que los datos personales deben tratarse de manera justa y lícita, los responsables del tratamiento de datos sobre niños deben respetar de forma aún más rigurosa el principio de minimización de datos y limitación de la finalidad.
>
> Concretamente, los responsables del tratamiento no deben procesar los datos sobre niños con fines de publicidad comportamental, ni directa ni indirectamente, por quedar esto fuera del ámbito de comprensión del niño y, por tanto, exceder los límites de tratamiento lícito.
>
> Los desarrolladores de aplicaciones, en colaboración con las tiendas de aplicaciones y los fabricantes de sistemas operativos y dispositivos, deben presentar la información pertinente de manera sencilla y con un lenguaje propio de las edades en cuestión.
>
> Asimismo, los responsables del tratamiento de datos deben abstenerse específicamente de toda recogida de datos sobre los padres o familiares del niño usuario, como información financiera o de categorías especiales de información, como los datos médicos.»

Como se ve, parece clara la preocupación por el tratamiento adecuado de los datos de los menores de edad. Es muy importante la información que se les da y cómo se les da, así como el consentimiento de los padres y tutores cuando no tienen la edad legalmente establecida para darlo ellos mismos, como se verá en los ejemplos de resoluciones de la AEPD sobre la materia. El tratamiento de imágenes de menores, el uso de las redes sociales, la dificultad que en ocasiones hay para establecer la edad real de los menores, son aspectos que no facilitan la cuestión.

Por lo que se refiere a la protección de datos y el consentimiento de los menores, el RGPD se refiere específicamente a la protección de datos de menores, lo que hasta ahora había hecho 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 Protección de Datos de Carácter Personal, estableciendo el límite de edad a los efectos de prestar el consentimiento en los 13 años. Ahora, el RGPD dedica el artículo 8 a la protección de datos de menores. Se refiere, más concretamente, a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información. Cuestión que engarza perfectamente en la materia que se está analizando, aunque Piñar Real entiende que este artículo 8 se podría aplicar también a otros supuestos que no fueran propiamente servicios de la sociedad de la información. Según el mencionado artículo:

> «1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.
>
> Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.»

Aquí se plantean varias cuestiones:

- La regulación actual de la edad en materia de protección de datos.
- La edad necesaria para la contratación en el caso de servicios de la sociedad de la información.
- La obtención del consentimiento de los padres o tutores en el caso en el que este es necesario.

Se puede ver que el límite de los 16 años puede coincidir con la edad de un menor emancipado que tendría capacidad para contratar, según el Código Civil, aunque obviamente no coincide con lo establecido en el Reglamento, ya que solo establece el límite de la edad para prestar consentimiento al tratamiento de datos de carácter personal. Según este artículo, un menor de 16 años, aunque no esté emancipado, puede prestar su consentimiento al tratamiento de sus datos de carácter personal.

También es verdad que el RGPD da cierto margen a los Estados miembros, al permitirles establecer una edad por debajo de los 16 años, siempre que no sea menor de 13 años. Hay que recordar que el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la LOPDP, en su artículo 13 establece la edad para prestar el consentimiento para el tratamiento de datos de carácter personal en los 14 años, «salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela». Los menores de 14 años necesitan el consentimiento de los padres o tutores.

Referencia bibliográfica

A. Piñar Real (2016). «Tratamiento de datos de menores de edad». En Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (pág. 194).

Según el Anteproyecto de LOPDP, solo será válido el consentimiento de los menores para el tratamiento de sus datos de carácter personal si son mayores de 13 años. Lo establece en estos términos:

> «Artículo 8. Consentimiento de los menores de edad
>
> 1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años.
>
> Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.
>
> 2. El tratamiento de los datos de los menores de trece años solo será lícito si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.»

Este artículo 13 establece también que en ningún caso puede recabarse información sobre los demás miembros del grupo familiar, como los datos relativos a la actividad profesional de los padres, información económica, datos sociológicos u otros, sin el consentimiento de los titulares de estos datos. Lo que sí podrá recabarse es la información de identidad y dirección del padre, la madre o el tutor solo a los efectos de obtener la autorización.

La información dirigida a los menores debe ser adecuada, en un lenguaje fácilmente comprensible. En este punto hay que decir que algunas normas sobre protección de los consumidores ya consideran a los menores «consumidores especialmente vulnerables».

Sin embargo, no pueden obviarse las dificultades de poder comprobar la edad real del menor. El artículo 13.4 del Real Decreto 1720/2007, de desarrollo de la LOPDP, hace recaer sobre el responsable del fichero o tratamiento la necesidad de articular procedimientos que garanticen que se ha comprobado «de modo efectivo» la edad del menor y la autenticidad del consentimiento prestado por los padres, tutores o representantes legales.

Volviendo al Reglamento General de Protección de Datos, el artículo 8 antes citado no es el único que hace referencia a los menores de edad. De igual modo, la la «Guía del Reglamento General de Protección de Datos», publicada por la AEPD (disponible en: http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf), se refiere a los menores:

- En la regulación de los intereses legítimos del responsable como base legal para el tratamiento, se establece que no será aplicable cuando prevalezcan los derechos, las libertades o los intereses de los interesados que requieran protección de datos personales, especialmente cuando esos interesados sean niños.

- Al señalar que la información que se ofrece a los interesados en relación con el tratamiento o con el ejercicio de derechos deberá ser especialmente

concisa, transparente, inteligible y proporcionada, con lenguaje claro y sencillo cuando los interesados sean niños.

- En el contexto del derecho al borrado de los datos personales.

- Al establecer que las actividades de formación y sensibilización dirigidas a los niños deberán estar entre las prioridades de las autoridades de protección de datos.

El RGPD establece que los responsables del tratamiento hagan «esfuerzos razonables», teniendo en cuenta la tecnología disponible, para verificar el consentimiento de los menores o de sus padres o tutores (art. 8.2 RGPD).

En otro ámbito, el Código Ético de Confianza Online dedica varios artículos a la publicidad, al tratamiento de datos y a la protección de menores:

«**Artículo 34. Publicidad y protección de menores**

La publicidad difundida en medios electrónicos de comunicación a distancia no deberá perjudicar moral o físicamente a los menores y tendrá, por consiguiente, que respetar los siguientes principios:

a) Deberá identificar los contenidos dirigidos únicamente a adultos.

b) No deberá incitar directamente a los menores a la compra de un producto o servicio, explotando su inexperiencia o su credulidad, ni a que persuadan a sus padres o tutores, o a los padres o tutores de terceros, para que compren los productos o servicios de que se trate.

c) En ningún caso deberá explotar la especial confianza de los niños en sus padres o tutores, profesores u otras personas.

d) No deberá, sin motivo justificado, presentar a los niños en situaciones peligrosas.

Artículo 35. Contenidos sobre protección de menores

1.- Las entidades adheridas no presentarán en sus sitios web contenidos, declaraciones o presentaciones visuales ilícitas o que pudieran producir perjuicio mental, moral o físico a menores.

2.- En caso de que las entidades adheridas presenten en sus sitios web áreas o secciones dirigidas a mayores de edad que pudieran producir perjuicio mental, moral o físico a menores, dichas áreas o secciones deberán ser identificadas correctamente y de forma previa a la navegación.

Artículo 36. Tratamiento de datos de menores

1.- Para recoger datos o comunicarse con menores a través de medios de comunicación electrónica, las entidades adheridas a este Código deberán tener en cuenta la edad, el conocimiento y la madurez de su público objetivo. En ningún caso podrán recabarse de los menores datos relativos o relacionados con la situación económica o la intimidad de los otros miembros de la familia.

2.- Las entidades adheridas a este Código alentarán a los menores a obtener la autorización de sus padres, tutores o representantes legales antes de facilitar datos personales en línea (*online*), y establecer mecanismos que aseguren razonablemente, de acuerdo con el desarrollo de la tecnología, que han comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento de aquellos. Lo anterior no será necesario cuando la información sea solicitada a adolescentes, siempre que los términos en que se solicita su consentimiento estén redactados de forma que sean fácilmente comprensibles para ellos.

3.-Los padres o tutores podrán oponerse al envío de publicidad o información solicitada por los menores a su cargo, dirigiéndose para ello al responsable del fichero mediante un sistema que asegure su identidad.

4.-Además del respeto a la opción de los padres de limitar la recogida de estos datos *online*, las entidades adheridas a este Código limitarán la utilización de datos proporcionados por los menores con la única finalidad de la promoción, la venta y el suministro de productos o servicios objetivamente aptos para menores.

5.- En ningún caso podrán cederse los datos relativos a menores sin el previo consentimiento de sus padres o tutores. No será necesario recabar dicha autorización cuando la cesión sea solicitada a un adolescente, siempre que los términos en que se solicita su consentimiento estén redactados de forma que sean fácilmente comprensibles para ellos.

6.- Las entidades adheridas a este Código deberán ofrecer a los padres o tutores información acerca de cómo proteger en línea (*online*) la privacidad de sus hijos o pupilos, así como facilitarles mecanismos para ejercer los derechos de acceso, rectificación, cancelación y determinación de la finalidad sobre los datos de aquellos.

7.- Las entidades adheridas a este Código realizarán sus mejores esfuerzos para apoyar iniciativas que se realicen por parte de otros organismos de reconocido prestigio para ayudar a informar a los padres o tutores sobre cómo proteger en línea (*online*) la intimidad de sus hijos o pupilos, incluyendo información sobre herramientas de software y control de acceso para los padres, que impidan que los niños proporcionen su nombre, dirección y otros datos personales.»

Ejemplo. Facebook: privacidad y menores

«[...] informamos a los menores acerca de lo que conlleva publicar contenido de forma pública. También evitamos que la información confidencial, como los datos de contacto de los menores, el colegio donde estudian y su fecha de nacimiento, aparezca en las búsquedas de todos los usuarios. Además, tomamos las medidas necesarias para recordar a los menores que solo deben aceptar solicitudes de amistad de personas que conozcan.

Los menores y el etiquetado

Cualquier persona que pueda ver una publicación puede añadir etiquetas en la misma. Cuando alguien está etiquetado en una publicación, el público de la publicación puede ampliarse e incluir también a sus amigos. Tanto los menores como los adultos pueden utilizar la herramienta *Revisión de etiquetas* para aprobar las etiquetas que los usuarios añaden a sus publicaciones antes de que estas aparezcan. Por defecto, esta función está activada para los menores.

Los menores y los adultos también pueden activar la opción *Revisión de la biografía* para revisar publicaciones en las que están etiquetados antes de que estas aparezcan en su biografía. Si un menor u otro usuario están etiquetados en algún tipo de contenido y no están de acuerdo, pueden eliminar la etiqueta o pedir a la persona que les haya etiquetado que elimine la publicación.

¿Cómo funciona la configuración de la ubicación en el caso de los menores?

Dada la importancia que tiene plantearse si compartir la ubicación o no antes de hacerlo, especialmente en el caso de los menores, la opción de compartir la ubicación está desactivada para ellos por defecto. Cuando un adulto o un menor activa la opción de compartir la ubicación, incluimos un aviso permanente con el fin de recordarles que están compartiendo su ubicación.»

Se puede consultar el texto íntegro en: https://www.facebook.com/help/473865172623776/.

Algunas resoluciones de la AEPD en relación con el consentimiento de menores y el tratamiento de datos de carácter personal

Resolución de la AEPD R/01579/2016

«Con fecha de 30 de diciembre de 2015 tiene entrada en esta Agencia un escrito de D. C.C.C. (en lo sucesivo el denunciante) comunicando que D. B.B.B. (en lo sucesivo el denunciado), se anuncia en Facebook, utilizando una foto en la que aparece la hija del denunciante y sus amigos, todos ellos menores de edad, sin tener autorización para dicha publicación. Adjunta a su denuncia, copia impresa de la publicación en

el perfil de FACEBOOK "***FACEBOOK.1", con fecha 24 de noviembre de 2015, de una fotografía en la aparecen varios menores sobre una tabla de surf, en dicho perfil se promociona la Escuela de Paddle Sup: "***FACEBOOK.1" con los datos para información y reservas de: "B.B.B.", Tfno: D.D.D. También se publica una dirección de correo electrónico y una página web.

La resolución impugnada razona pormenorizadamente sobre la existencia de tratamiento automatizado de datos de carácter personal de los menores, sus imágenes, sin que en la demanda se suscite cuestión alguna sobre dichos extremos, no ofreciendo dudas a la Sala la existencia del tratamiento de datos de carácter personal de los menores dado el amplio concepto de tratamiento de datos que ofrece el artículo 3.c) LOPD y 5.1.t) RLOPD. Debe señalarse que la Directiva 95/46/CE es aún más minuciosa en la enumeración de las operaciones o procedimientos que constituyen tratamiento: recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como bloqueo, supresión o destrucción.

Y en el presente caso la divulgación por medio de video de la imagen de los menores, constituye un tratamiento de sus datos de carácter personal, que al ser menores de 14 años de edad, pues contaban entre 7 y 8 años de edad, requiere para poder efectuarlo el consentimiento de sus padres o tutores, como exige el artículo 13.1 del RLOPD en relación con el artículo 6 LOPD que regula el principio del consentimiento para el tratamiento de los datos de carácter personal del afectado. Por tanto, las alegaciones referentes a si los menores no se encontraban acompañados por sus profesoras en el concreto momento en que se grababa el video, resultan irrelevantes a los efectos del presente procedimiento, pues los menores por su edad no podían consentir ni la grabación ni la difusión de su imagen y el citado artículo 6.1 de la LOPD dispone, con carácter general, que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

Cabe resaltar que la imagen del menor tiene una consideración legal especialmente protectora, como ha señalado la STS, Sala 1ª, de 13 julio 2006 (Rec. 2947/2000) tras referirse a su jurisprudencia y a lo dispuesto en los arts. 18.1 y 20.1 CE, los arts. 2.2, 3, 7.5 y 8.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y el art. 4.1 de la Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor.»

Resolución de la AEPDR/00910/2017 (disponible en: http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2017/common/pdfs/A-00512-2016_Resolucion-de-fecha-07-04-2017_Art-ii-culo-6-LOPD.pdf)

«En el presente caso, RECIO FOTOVÍDEO es responsable de la exposición en su establecimiento de la fotografía efectuada a la menor, que fue objeto de denuncia, y por lo tanto es la responsable del tratamiento del dato personal de su imagen, requiriéndose para el mismo el consentimiento de los padres; sin que RECIO haya acreditado la obtención del mismo. El artículo 44.3.b) de la LOPD, tipifica como infracción grave: "Tratar los datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta Ley y sus disposiciones de desarrollo".

Tomando en consideración los anteriores hechos y fundamentos de derecho, cabe concluir que RECIO FOTOVÍDEO trató sin consentimiento los datos personales de la menor lo cual constituye la referida infracción del artículo 6.1 de la LOPD.»

Resolución de archivo de actuaciones de la AEPD. Expediente: E/02689/2016

En este caso se archivan las actuaciones al quedar probado que, a pesar de ser un contrato de telefonía realizado por un menor de 14 años, consta el consentimiento de la madre. Sobre el consentimiento del menor apunta que: «el consentimiento para el tratamiento de los datos personales solamente puede ser otorgado por el interesado, salvo en el caso de que el afectado sea menor de 14 años o incapaz, en cuyo caso deber ser otorgado por sus padres o tutores, sin perjuicio de que estos deban completar la capacidad del menor, aunque sea mayor de 14 años, en aquellos supuestos en que una Ley así lo establezca».

Resolución de la AEPD 553/2004

«Los hechos son los siguientes: Telefónica y Megatrix suscribieron con fecha de 31 de octubre de 2002 un contrato con objeto de llevar a cabo una campaña publicitaria consistente en ofertar productos y servicios de telecomunicaciones de Telefónica a los

socios del club infantil Megatrix. Entre los destinatarios de la campaña, se encuentra R.G.H., cuyos datos han sido obtenidos por Megatrix del propio interesado en soporte papel, mediante un cupón de suscripción como socio al Club Megatrix firmado por los padres/tutor del propio interesado. La cláusula sobre la que se discute tiene el siguiente tenor literal: "La finalidad de este fichero es mantener la relación con los socios del Club Megatrix, para comunicarles actividades culturales, formativas, deportivas y de ocio y para el envío de promociones comerciales de productos y servicios que puedan resultar de su interés. Además los datos correspondientes a los representantes legales del socio podrán utilizarse, conjunta o separadamente, para informarles de otras actividades complementarias de las descritas y de similar naturaleza y finalidad, pero dirigidas a personas adultas. MEGATRIX podrá ceder los datos del fichero a otras empresas dedicadas a estos mismos fines. El ejercicio de los derechos de acceso, rectificación, oposición y cancelación regulados en la LOPDP deberá realizarse en la dirección antes indicada". La pregunta que hay que formular es la siguiente: ¿Es suficiente lo establecido en esta cláusula como consentimiento para el tratamiento de datos de carácter personal para fines publicitarios o promocionales de productos de "Telefónica"? La respuesta es negativa. El tenor de la cláusula transcrita, según la AEPD, no solo no informa en los términos legalmente exigibles sino que más bien los invierte al obligar al afectado a manifestar por escrito su deseo de no recibir unas comunicaciones respecto de las que no se le ha informado de forma determinada y explícita: "La leyenda no cumple con las exigencias de haber facilitado previamente una información expresa, precisa e inequívoca (art. 5 LOPDP) sobre las finalidades determinadas y explícitas para las que se recabaron y trataron los datos (art. 4.1)". Se condena a Megatrix por una infracción grave al pago de 60.101,21 euros.»

Es importante diferenciar el consentimiento para el tratamiento de datos personales del menor, de acuerdo con la edad establecida en el RGPD o, en su caso, la que establezcan los Estados dado el margen que en este tema otorga el Reglamento, de la edad en que puede contratar, que dependerá de las normas sobre capacidad y contratación del Código civil.

Otra cuestión a la que hay que hacer referencia es al uso de las redes sociales por parte de los menores. El«Dictamen 5/2009 sobre las redes sociales en línea» del Grupo de Trabajo del Artículo 29 (disponible en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf), adoptado el 12 de junio de 2009, se refiere a los peligros que puede suponer para los menores el uso de las redes sociales, teniendo en cuenta el gran número de ellos que las utilizan. Según este dictamen, sería adecuada una estrategia pluridimensional para abordar la protección de datos de los niños en las redes sociales. Esta estrategia se basaría en:

- Iniciativas de sensibilización, fundamentales para garantizar el compromiso activo de los niños (mediante las escuelas, la inclusión en el programa escolar de elementos de protección de datos, la creación de herramientas educativas *ad hoc* y la colaboración de organismos nacionales competentes).

- Un tratamiento justo y legal frente a los menores, como por ejemplo, no pedir datos sensibles en el formulario de registro, no realizar comercialización directa destinada específicamente a los menores, el acuerdo previo de los padres antes del registro, así como grados adecuados de separación lógica entre las comunidades de niños y de adultos.

- La instauración de tecnologías que mejoren la protección de la intimidad, es decir, parámetros por defecto respetuosos de la intimidad, ventanas emergentes de advertencia en fases adecuadas, así como programas informáticos de verificación de la edad.

- La autorregulación de los proveedores con el fin de fomentar la adopción de códigos de buenas prácticas que deberían incluir medidas de ejecución eficaces y sanciones disciplinarias.

- En caso necesario, medidas legislativas *ad hoc* para desalentar prácticas desleales y/o fraudulentas en el contexto de las redes sociales.

Entre las principales dificultades, está la de comprobar que realmente se trata de un menor. Junto a las normas, serían necesarias herramientas tecnológicas para poder comprobar realmente la veracidad de los datos correspondientes a la fecha de nacimiento.

Lectura recomendada

Sobre este tema, véase:

E. Díaz Díaz (2016). «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones». *Revista Aranzadi Doctrinal* (núm. 6/2016, BIB 2016\3067).

Bibliografía

Básica

Díaz Díaz, E. (2016). «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones». *Revista Aranzadi Doctrinal* (núm. 6/2016, BIB 2016\3067).

Varios autores (2009). *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPDP*. Valencia: Tirant lo Blanch.

Específica

Álvarez Hernando, J. (2014). «Publicidad, comunicaciones comerciales y protección de datos». En: *Practicum de Protección de Datos 2015*. Cizur Menor: Aranzadi.

Aparicio Salom, J.; Sanfulgencio Tomé, S. (2014). «El régimen jurídico de las *cookies* y su aplicación por la Agencia Española de Protección de datos». *Revista Aranzadi Doctrinal* (núm. 11/2014. BIB 2014\675).

Camacho Clavijo, S. (2016). «Régimen jurídico de los prestadores de servicios de la sociedad de la información». En: Navas Navarro, S.; Camacho Clavijo, S. *Mercado Digital. Principios y reglas jurídicas*. Valencia: Tirant Lo Blanch.

Cavanillas Múgica, S. (2011). «Comentario a la Sentencia del Tribunal Supremo de 18 de mayo de 2010: responsabilidad de un prestador de un servicio intermediario de la sociedad de la información, de alojamiento, por la intromisión ilegítima causada por un comentario enviado a un foro». *Revista Cuadernos Civitas de Jurisprudencia Civil* (núm, 85, págs. 447-456).

de Miguel Asensio, P. A. (2015). «Prácticas desleales y comunicaciones comerciales». En: de Miguel Asensio, P. A. *Derecho Privado de Internet*. Cizur Menor: Westlaw (BIB 2015\7).

Duaso Calés, R. (2016). «Los principios de protección de datos desde el diseño y la protección de datos por defecto». En: Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (págs. 295-333).

Grimalt Servera, P. (2005). «Deberes y responsabilidades en materia de protección de datos». En: Cavanillas Múgica, S. (coord.). *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares (págs. 183-201).

Navas Navarro, S. (2016). «*Cookies* y tecnología análoga: publicidad comportamental online y protección de los datos de carácter personal». En: Navas Navarro, S.; Camacho Clavijo, S. *Mercado Digital. Principios y reglas jurídicas*. Valencia: Tirant lo Blanch (pás. 357-380).

Paniza Fullana, A. (2004). «Comunicaciones comerciales no solicitadas y marketing directo: el sistema *opt out* como excepción. Correo Electrónico y mensajes SMS con fines publicitarios». *Avances en Criptografía y Seguridad de la Información*. Madrid (págs. 437-445).

Paniza Fullana, A. (2010). «Alcance de la responsabilidad de los prestadores de servicios de la sociedad de la información. (A propósito de la Sentencia del Tribunal Supremo de 18 de mayo de 2010.)». *Aranzadi Civil. Revista Doctrinal* (núm. 4, págs. 27-36.

Paniza Fullana, A. (2009). «Cuestiones jurídicas en torno a las redes sociales: uso de datos personales para fines publicitarios y protección de datos de menores». *Revista Española de Protección de Datos* (núm. 6, págs. 41-68).

Payeras Capellà, M.; Cavanillas Múgica, S. (2005). «Los servidores de acceso y alojamiento: descripción técnica y legal». En: Cavanillas Múgica, S. (coord.) *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*. Granada: Comares (págs. 1-48).

Payeras Capellà, M.; Mut Puigserver, M.; Paniza Fullana, A.; Isern Deyà, A. P. (2014). «Privacidad en servicios turísticos basados en geolocalización». *Revista de Derecho, Empresa y Sociedad (REDS)* (núm. 5, ISSN: 2340-4647, págs. 78-93).

Peguera Poch, M. (2007). *La exclusión de responsabilidad de los intermediarios en Internet*. Granada: Comares.

Piñar Mañas. J. L. (2016). «Introducción. Hacia un nuevo modelo europeo de protección de datos». En: Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (págs. 15-22).

Piñar Real, A. (2016). «Tratamiento de datos de menores de edad». En Piñar Mañas, J. L. (dir.). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus (págs. 187-203).

Troncoso Reigada, A. (2012). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales». *Revista de Internet, Derecho y Política* (núm. 15, págs. 61-75).

Varios autores (2010). *Publicidad, defensa de la competencia y protección de datos*. Cizur Menor: Aranzadi.

Vilasau Solana, M. (2008). «¿Cómo llegar al consumidor? Entre la protección de datos y la legislación sobre la sociedad de la información». *Revista Aranzadi de Derecho y Nuevas Tecnologías* (núm. 3, págs. 83-101).

Vilasau Solana, M. (2011). «Consentimiento, fuentes accesibles al público e interés legítimo como mecanismos que legitiman el tratamiento de datos de carácter personal». En: Blasco Gascó, F. y otros (coords.). *Estudios jurídicos en homenaje a Vicente L. Montés Penadés*, tomo II. Valencia: Tirant lo Blanch (págs. 2877-2898).

Enlaces

https://responsabilidadinternet.wordpress.com/.

http://www.agpd.es/portalwebAGPD/resoluciones/index-ides-idphp.php.

http://www.agpd.es/
portalwebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf.

http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf.

http://ec.europa.eu/
justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.