INTIMIDAD PERSONAL, PROTECCIÓN DE DATOS PERSONALES Y GEOLOCALIZACIÓN

Personal Privacy, Personal Data Protection and Geolocation Apps

ALFREDO BATUECAS CALETRÍO
Profesor Contratado Doctor
Universidad de Salamanca

Recepción: 25/02/2015
Aceptación después de revisión: 28/07/2015
Publicación: 27/11/2015

RESUMEN

La geolocalización, aplicación de uso común incorporada en los teléfonos móviles actuales, puede terminar vulnerando la intimidad de las personas. En este artículo se estudia cómo el derecho fundamental a la intimidad personal y el derecho fundamental a la protección de datos constituyen límites que no deben excederse con el uso de esta nueva aplicación tecnológica, así como la importancia que tiene el consentimiento prestado por el propietario del dispositivo en lo relativo al modo en que la aplicación de geolocalización debe realizar el tratamiento de sus datos personales.

PALABRAS CLAVE: Geolocalización; teléfono móvil; intimidad personal; protección de datos.

ABSTRACT

Geolocation, commonly used application on currents mobile phones, could end up damaging the privacy of individuals. This article study how the rights to privacy and data protection are limits that must not be exceed with the use of this new technological application, as well as the importance of the consent given by

the owner of the device with regard to how the geolocation application should perform the processing of personal data.

KEY WORDS: Geolocation; mobile phone; privacy; data protection.

I. INTRODUCCIÓN

La geolocalización, entendida como la tecnología que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento, debe ser objeto de estudio por el Derecho en orden a los posibles riesgos que su uso puede implicar para la persona física, especialmente en el ámbito de su intimidad personal[1].

Hoy día contienen aplicaciones de geolocalización la práctica totalidad de los dispositivos móviles inteligentes (*smartphones*, *tabletas*, navegadores de los automóviles, etc.), además de los ordenadores personales de sobremesa; utilizándose esta tecnología con las funciones más diversas (personales, laborales o de ocio). La geolocalización permite calcular la ruta que debe seguirse para llegar a una población, localizar un lugar en el mapa de coordenadas, incorporar a una fotografía las coordenadas del lugar en que fue tomada (lo que se conoce como «geoetiquetado»)[2], remitir publicidad[3] o se solicita como requi-

---

[1] Este artículo ha sido realizado dentro del marco del Proyecto de investigación «Privacidad y redes sociales: nuevos retos en la protección de datos y de los derechos al honor, intimidad e imagen» (Ref. DER2013-42294-R), financiado por el Ministerio de Educación y Ciencia, siendo investigador principal del mismo Juan Pablo Aparicio Vaquero.

El posicionamiento de un dispositivo en la Tierra se obtiene a partir de la latitud y la longitud que ocupa, siendo estas las coordenadas que miden el ángulo entre un punto cualquiera y su referencia (el ecuador para la latitud y el meridiano de Greenwich para la longitud).

[2] La mayoría de los teléfonos móviles actuales lo hacen automáticamente, si está activada esta aplicación.

Junto al de geoetiquetado, otros conceptos cuyo uso también es común en el argot técnico son el de «georreferenciación», para aludir al proceso de definición de una persona o un objeto en un espacio físico mediante el cálculo de su localización en un sistema de coordenadas; y el de «geocodificación», referido a la búsqueda de información y su localización física en un sistema de coordenadas.

[3] Técnica o práctica esta consistente en mostrar en el dispositivo puntos comerciales cercanos (tiendas, restaurantes, cines, etc.) que pueden resultar de interés en atención a gustos y preferencias previamente conocidos, por ejemplo, por haber visitado ciertas páginas web. Son aplicaciones de este tipo *Bliquo*, *Buzzd* o *Google Places Directory*. Esta práctica se denomina «publicidad orientada por los comportamientos».

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

sito necesario para poder participar en nuevas redes sociales (tipo *Foursquare)*[4].

Aunque las ventajas que proporciona la geolocalización son evidentes, su uso no está exento de inconvenientes o riesgos[5], siendo el principal de todos ellos la vulneración en su intimidad que puede sufrir la persona física[6]. La afección de la intimidad es resultado, por una parte, de la tendencia generalizada que existe entre los usuarios de los dispositivos móviles de mantener estos aparatos muy cerca de ellos (especialmente el teléfono móvil), estableciéndose un vínculo de proximidad estrecho entre la persona y el dispositivo[7] y, por otra parte, del desarro-

---

[4] Estas redes se utilizan por los usuarios con distintos propósitos: localizar a amigos o dar a conocer su ubicación (*Facebook places*, *Twitter places*); compartir opiniones, comentarios o experiencias con personas que se encuentran en un mismo punto geográfico (*Dopplr*); obtener información relativa a sitios de ocio (*Bliquo*), servicios públicos u organismos oficiales (*AroudMe*, *Buzzd*), a requerimiento (*Google maps*, *Foursquare*).

[5] En otros, remisión de publicidad en forma de *spam*, tarificaciones de servicios que se creían no contratados, etc.

[6] Sobre cómo pueden afectar las nuevas tecnologías en general (no limitadas al caso concreto de la geolocalización), de uno u otro modo, a la intimidad personal *vid*., entre otros, Cabello Fernández, M. D. «Protección de datos e internet», *RCE. Revista de la Contratación Electrónica*, n.º 116, noviembre-diciembre 2011; Davara Rodríguez, M. Á. «El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho», en *Diario La Ley*, n.º 8157, 26 de septiembre de 2013. De este mismo autor véase también «Intimidad, protección de datos y seguridad: un difícil equilibrio», en *Diario La Ley*, n.º 7276, 4 de noviembre de 2009; Gil Antón, A. M. «La privacidad del menor en internet», en *R.E.D.S*. n.º 3, septiembre-diciembre 2013; Grimalt Servera, P. «Los menores e internet: capacidad *versus* protección de la vida privada», en *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa* (coords. Cuena Casas, Anguita Villanueva, Ortega Doménech), Madrid, Ed. Dykinson, 2013; Megías Terol, J. «Privacy by design, construcción de redes sociales garantes de la privacidad», en *Derecho y redes sociales* (editores Rallo Lombarte y Martínez Martínez). Segunda edición. Ed. Civitas Thomson Reuters, 2013; Orozco Pardo, G. «Intimidad, privacidad, "eximidad", y protección de datos del menor. ¿Un cambio de paradigma?», en *La protección jurídica de la intimidad* (coords. Javier Boix Reig, Ángeles Jareño Leal), Ed. Iustel, Madrid, 2010; Paniza Fullana, A. «Problemática jurídica del menor como consumidor/usuario en la sociedad de la información», en *Congreso Derecho y Nuevas Tecnologías*, Universidad de Deusto, Bilbao, 2009; Pérez Luño, A. E., «La protección de los datos personales del menor en internet», en *Anuario Facultad de Derecho de la Universidad de Alcalá*, 2009; Piñar Mañas, J. L. «El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales», en *Redes sociales y privacidad del menor*. Editorial Reus, 2011.

[7] Debido a que una gran cantidad de información que contienen los dispositivos móviles es privada (como fotografías, mensajes, lista de contactos, etc.), no es común que una persona preste, por ejemplo, su teléfono móvil a otra.

llo tecnológico actual, que posibilita una localización permanente de los terminales y, al mismo tiempo, la identificación directa y rápida del propietario del dispositivo[8]. Basta solo con poner en relación los datos de posicionamiento de un terminal con el de quien ostenta su propiedad para llegar a conocer detalles de la vida de las personas. Como apunta Barinas Ubiñas, la geolocalización propicia la confección de «perfiles y patrones de comportamiento» que van horadando las barreras de lo que representa la idea de privacidad desde una reconfiguración de la identidad y personalidad del ser humano, ahora representada, dentro de este entorno digital, a través de datos que se interconectan[9].

La vulneración de la intimidad de las personas físicas a consecuencia del uso de la geolocalización preocupa a nivel nacional, como puede comprobarse en múltiples resoluciones de la Agencia Española de Pro-

---

[8] En el trabajo se partirá siempre del presupuesto de que el «usuario» del teléfono es su «propietario», utilizando ambas expresiones como sinónimas, en atención a que esta es la situación que acontece con mayor frecuencia en la vida real. Siendo esto así, es preciso acotar que puede suceder también que quien esté utilizando el dispositivo no sea su propietario, sino una persona distinta. Cuando así ocurra, la intimidad personal que se verá afectada será la del propietario del dispositivo, por ser la localización del terminal la que se transmite y ser suyos los datos que están asociados al terminal. Por último, en el supuesto concreto del geoetiquetado, pudiera suceder que quien transmite los datos no sea el titular del dispositivo y que, a mayores, la persona de quien se transmiten los datos (por aparecer en la fotografía) sea distinto de los otros dos.

[9] BARINAS UBIÑAS, D. «El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada», en *Revista Electrónica de Ciencia Penal y Criminología*, 15-09 (2013), p. 4. En igual sentido, véase CAMPUZANO TOMÉ (*Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*. Madrid: Ed. Tecnos, 2000, p. 69), quien, refiriéndose a los nuevos medios electrónicos, señala que estos no han modificado el concepto de privacidad, sino que han cambiado las formas en que esta puede ser protegida o puesta en peligro.

El «patrón de conducta» alude al perfil de la persona que se obtiene después de relacionar todos los datos de posicionamiento que haya emitido su dispositivo en un intervalo de tiempo (diariamente, semanalmente, mensualmente, etc.). El hecho de que la mayoría de estos dispositivos tenga capacidad de almacenamiento y que baste sencillamente con acudir a su memoria para conocer cuáles fueron las últimas operaciones que se realizaron con él permite que pueda definirse su personalidad y sus tendencias de comportamiento. Tecnológicamente es factible acceder a la información tratada por un GPS incluso después de que haya sido borrada de este. Según VELASCO NÚÑEZ («Tecnovigilancia, geolocalización y datos: aspectos procesales penales». En *Diario La Ley*, n.º 8338, Sección Doctrina, 23 de junio de 2014, p. 3), estos perfiles que se crean sobre datos que aislados parecen inocuos, pero que convenientemente tratados vulneran nuestra privacidad, están obligando al Derecho a reinterpretar la necesidad de protegernos de ese plus de ingerencia en la privacidad que aportan las máquinas.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

tección de Datos (en adelante, AEPD)[10], y a nivel europeo, como se pone de manifiesto en el Dictamen aprobado por el Grupo de Trabajo del artículo 29, el 16 de mayo de 2011, referido a los servicios de geolocalización en los teléfonos móviles[11] o en la sentencia del TEDH, caso *Uzún vs Alemania*, Secc. 5.ª, de 2 de septiembre de 2010 (asunto 35625/05), en la que el Tribunal concluye que una geolocalización continua afecta a la vida privada[12].

---

[10] Cada vez es mayor el número de casos sobre los que está conociendo la AEPD. Así, a modo de ejemplo, sin pretender ser exhaustivos y aparte de otras Resoluciones que se citan a lo largo del trabajo y que demuestran que esto es así, solo en los dos últimos años la AEPD se ha visto obligada a conocer sobre asuntos de geolocalización en las Resoluciones: R/00520/2015; R/02531/2014; R/01208/2014, R/02761/2013, R/00956/2013, así como en los Expedientes E/04153/2014, E/02994/2014, E/07134/2013. Igualmente, ha tenido que pronunciarse a resultas de las consultas que se le plantean en el Informe Jurídico 0071/2013.

Debe destacarse que un alto porcentaje de estos asuntos están referidos al uso de la geolocalización en el entorno laboral (en particular, la instalación de gps en automóviles de la empresa), siendo coincidente en muchos de ellos que el empresario no ha informado acerca de su instalación a los trabajadores o cuando, habiendo informado, utiliza los datos de localización para una finalidad distinta de aquella sobre la que informó. Sin duda alguna, las sanciones impuestas por la AEPD cuando esto ha sido así, por vulneración del artículo 5 LOPD, hará que cada vez sea más extendido entre las empresas el cumplimiento del deber de información al que obliga dicho precepto.

[11] Ref. 881/11 (WP 185).

El Grupo de Trabajo del artículo 29 es un órgano de carácter consultivo formado por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. El Grupo examina cualquier cuestión relacionada con la aplicación de las directivas en materia de protección de datos. Desempeña sus funciones emitiendo Recomendaciones, Dictámenes y documentos de trabajo sobre todas aquellas cuestiones relevantes que afectan a la protección de datos personales.

[12] En correspondencia con lo que ya desde hace algunos años viene apuntando la Comisión Europea, para quien la rapidez de la evolución tecnológica y la globalización han modificado profundamente nuestro medio y han lanzado nuevos retos en materia de protección de datos personales (véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre un enfoque global de la protección de los datos personales en la Unión Europea, de 4 de noviembre de 2010 (COM(2010) 609 final). Ha sido la protección de datos en el entorno digital lo que ha motivado que la Comisión Europea haya promovido la modificación de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, presentado al Parlamento Europeo una Propuesta de Reglamento de Protección de Datos [véase Propuesta de Reglamento del Parlamento Europeo y del Consejo 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, de 25 de enero de 2012, COM (2012) 11 final], cuya aprobación,

En atención al concepto amplio de dato personal que se consagra en el artículo 3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), la información de posicionamiento del terminal debe considerarse dato personal. En dicho precepto, sin precisar más y con afán claro por parte del legislador de proteger en la mayor medida posible a la persona, se indica que dato de carácter personal es «cualquier información concerniente a personas físicas identificadas o identificables». En aras de comprender verdaderamente su alcance, este precepto debe ser puesto en relación con el artículo 5.1.f) del Real Decreto 1720/2007, que aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (en adelante, RLOPD), un poco más clarificador que el anterior, aunque solo sea por la ejemplificación que en él se realiza. En concreto, en este otro artículo se describe al dato personal como «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables».

Es en virtud de la parte final del precepto, en concreto cuando se refiere a personas físicas «identificables», por la que el dato de geolocalización debe considerarse dato personal. La información de posicionamiento, sin ser alfabética, gráfica o fotográfica, que es la información por la que de forma directa más fácilmente se identifica a un individuo, también sirve para identificar a una persona. Si bien en un inicio la información de posicionamiento de un terminal, por sí misma, no identifica de forma inmediata o directa a una persona, sin embargo sí puede terminar haciéndolo de forma mediata o indirecta, desde el momento que está referida al dispositivo que la persona comúnmente porta consigo. Basta con poner en relación o «cruzar» el dato de posicionamiento del terminal con el de quien es su propietario para que a partir del dato de posicionamiento se pueda identificar a una persona y se pueda obtener información personal de un individuo (en qué lugar ha estado, a qué hora ha estado en ese lugar, de dónde venía, a qué lugar fue después, etc.), como se aclara en la Resolución R/02761/2013 de la AEPD. Téngase en cuenta en este punto, por una parte, que cada terminal se identifica con una dirección numérica única y, por otra, que, según la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (modificadora de la Directiva 2002/58/CE relativa al tratamiento de los datos persona-

---

si finalmente se produce, obligará a introducir modificaciones en las legislaciones nacionales de protección de datos de los diferentes Estados.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

les y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que es la que hasta entonces definía el dato de localización), el dato de localización es «cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público»[13].

Cruzar los datos de posicionamiento con el de la titularidad del dispositivo (a partir de las bases de datos de los abonados de las compañías telefónicas) es una actividad relativamente fácil desde el punto de vista tecnológico para cualquiera con ciertos conocimientos informáticos y una práctica común en algunos sectores como el de los servicios de urgencias o los cuerpos de seguridad del Estado, como puede comprobarse en el Informe 0071/2013 de la AEPD, en el que se detalla el funcionamiento del servicio de urgencias de una Comuni-

[13] A este respecto, el estudio de las Directivas aplicables resulta mucho más complejo que el de la normativa estatal. En principio, por la materia, podrían resultar aplicables tres Directivas: 1) la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; 2) 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 posteriormente por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n.º 2006/2004 sobre la cooperación en materia de protección de los consumidores; y 3) la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco).

Debe advertirse que la Directiva 2002/58/CE no se aplicará al tratamiento de los datos de geolocalización cuando dicho tratamiento lo haya realizado una empresa que actúe como prestador de servicios de la sociedad de la información, por estar excluidos explícitamente estos prestadores del ámbito de los servicios de las comunicaciones electrónicas, en virtud de la definición estricta de «servicios de comunicaciones electrónicas» que establece la Directiva 2002/21/CE (art. 2. Letra c), Directiva Marco. Esto significa que en todos aquellos casos en los que el usuario elija transmitir los datos de posicionamiento a través de internet (por ejemplo, cuando acceda *on line* a una aplicación web de geolocalización), y no por la red GSM, no resultará de aplicación la Directiva 2002/58/CE. Sobre la no aplicación de la Directiva 2002/58/CE cuando la transmisión de datos se realice por internet, véase el Dictamen 13/2011 del Grupo de Trabajo del artículo 29, sobre los servicios de geolocalización en los dispositivos móviles, p. 9.

dad Autónoma y como este cruza automáticamente los datos del terminal con el de la titularidad del mismo cada vez que recibe una llamada de urgencia[14].

A estos efectos, el dato de posicionamiento debe recibir un tratamiento semejante al de la dirección IP de un ordenador personal, que ha sido considerada dato de carácter personal por la AEPD, en atención a la estrecha vinculación que el dato de esa naturaleza guarda con el terminal. En este sentido, lo que se expone en el Informe Jurídico 327/2003 de la AEPD con respecto a la IP de un ordenador personal entendemos que es trasladable al dato de posicionamiento de un terminal, pues tanto en un caso como en otro «por medios razonables» es posible llegar a identificar al titular de un terminal (que, en suma, es lo que justifica que a la IP se le considere dato personal). Es más, en el caso del dato de localización puede llegar a ser incluso más sencillo que en el de la IP, ya que en él el número desde el que se emite el dato es siempre el mismo (el del terminal), no existiendo aquí el problema de las IP dinámicas que sí puede darse en el del ordenador personal. La clave en uno y otro caso es que a partir de ese dato (la IP o el dato de localización) por medios razonables se puede llegar a identificar a una persona.

Como consecuencia de lo que se acaba de señalar, parece claro que es importante garantizar la protección de datos en el sector de la geolocalización[15].

---

[14] Sin perjuicio de que esta labor de puesta en relación de los datos de posicionamiento con los de la titularidad del terminal es posible realizarla a partir de programas informáticos que cualquiera puede obtener en internet y de que existen empresas que prestan estos servicios, lo será especialmente para la compañía telefónica que presta el servicio de telefonía al titular del terminal, ya que esta compañía conoce el terminal desde el que se envía la señal de posicionamiento y tiene acceso a los datos personales de la persona a quien pertenece el terminal. Piénsese, sin ir más lejos, que la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, aunque solo sea a efectos de su posterior facturación.

[15] Una protección adecuada repercutirá, a su vez, en una mayor confianza de los usuarios en estos servicios. Como se afirma en el Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Un enfoque global de la protección de los datos personales en la Unión Europea» (DOCE C 181/01, de 22 de junio de 2011), p. 3, parágrafo 21, aunque referido a las nuevas tecnologías en general, los ciudadanos no delegarán su confianza mientras no perciban que sus datos se encuentran adecuadamente protegidos. Véase, en igual sentido, el Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad (DOCE C 280/01, de 26 de octubre de 2010).

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

II. EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL Y FAMILIAR Y EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS COMO LÍMITES EN EL USO DE LA GEOLOCALIZACIÓN

El mayor peligro que presenta la geolocalización, como ya se ha apuntado, es la posibilidad de que con su uso pueda vulnerar la intimidad de las personas. Piénsese que por medio de esta tecnología es posible llegar a conocer aspectos de la vida de la persona relativos a los lugares a los que asiste regularmente (hospitales, sedes políticas, sindicatos, etc.), a sus gustos (por los establecimientos de ocio o compras que visita) o a las horas a las que accede a los mismos[16].

La geolocalización deviene igualmente intrusiva si, utilizándose con una finalidad concreta (por ejemplo, calcular una ruta de destino), los datos se tratan posteriormente con un objetivo distinto (por ejemplo, remitir publicidad de locales comerciales cercanos o ejercer algún tipo de control o vigilancia sobre los trabajadores de una empresa)[17].

---

[16] Si se analiza el resultado de los últimos usos del GPS de un turista viajero se tendrá acceso, no solo a la ruta que ha seguido, sino también a todos los lugares que hayan quedado marcados como de su gusto.

[17] En este sentido, comienzan a ser ya numerosos los supuestos de uso de geolocalización en el ámbito laboral para obtener fines no permitidos, derivando en una técnica invasiva para el trabajador. Ocurre esto cuando se instalan GPS en los vehículos de los empleados sin informar previamente sobre ello o cuando, habiendo informado a los trabajadores, los GPS se utilizan con una finalidad distinta de la que inicialmente se declaró a la AEPD cuando se dio de alta el fichero. El uso de GPS en los vehículos de una empresa exige informar previamente a los trabajadores de la misma, ya que los datos de posicionamiento que se tratarán estarán referidos a ellos y cualquier tratamiento de datos exige el consentimiento previo del interesado (art. 6 LOPD). En estos casos, el uso de los GPS, además de estar justificado, deberá ser lo menos intrusivo posible en la esfera personal del trabajador (por ejemplo, respetando sus tiempos de descanso).

La mayoría de las Resoluciones resultantes de expedientes sancionadores incoados por la AEPD en estos supuestos han fundamentado la decisión de sancionar la infracción cometida por el empresario al no informar previamente a los trabajadores de la instalación del GPS en el vehículo de la empresa. Un ejemplo se encuentra en la Resolución R/02761/2013, en la que la AEPD sigue un procedimiento sancionador contra la Dirección General de la Guardia Civil por un tratamiento ilegítimo de datos obtenidos de los GPS instalados en sus coches-patrulla, por cuanto la información remitida por el GPS estaba siendo utilizada al objeto de controlar y vigilar si la ruta de servicio que llevaban a cabo los guardias civiles que se encontraban de patrulla era correcta, sin haber informado previamente de ello a los guardias civiles. No concluyen con sanción, por haberse informado previamente a los trabajadores de la instalación del GPS, las Resoluciones correspondientes a los expedientes sancionadores n.º E/00742/2008, E/02689/2012 o E/04495/2012.

No obstante, los riesgos descritos no deben ser entendidos como una característica que acompaña de forma consustancial a la geolocalización y que irremediablemente hay que aceptar si se quiere disfrutar de los beneficios que aporta esta tecnología. Las vulneraciones de intimidad descritas se evitan con una regulación jurídica adecuada de protección de datos, que ampare a la persona física (se comienza a hablar de «derecho a no estar localizado»[18] o «derecho al anonimato»)[19], así como con la adopción de ciertos usos por parte de las compañías que operan con geolocalización. Respecto a estas compañías es preciso apuntar que la geolocalización les afecta de diferentes formas. Así, mientras que en unas compañías constituye el objeto del servicio que prestan (por ejemplo, aplicaciones de geolocalización que ubican al terminal en un mapa de coordenadas); en otras, sin ser exactamente el objeto del servicio que prestan, la geolocalización se utiliza indirectamente para prestar otros servicios (por ejemplo, aplicaciones que muestran el tiempo que hace en una determinada localidad).

La protección que debe recibir el titular de un terminal cuando se vulnera su intimidad con una aplicación de geolocalización se obtiene por medio del artículo 18 de la Constitución Española (en adelante, CE), precepto en el que después de consagrar en el párrafo primero a título general un derecho a la intimidad personal y familiar, dedica su párrafo cuarto a reconocer un derecho específico a la protección de datos personales[20]. El legislador confiere contenidos distintos a uno y otro

---

Sobre este tema concreto de la utilización del GPS en el entorno laboral, véase el Informe 0613/2009 de la AEPD, en el que la Agencia responde a diversas cuestiones planteadas por una empresa con respecto a la aplicación de la LOPD a un servicio de geolocalización del que dispone.

[18] Véase DESPACHO CREMADES & CALVO SOTELO «Estatuto jurídico de los servicios de radiolocalización —GPS— a través de redes de telefonía móvil —GSM—», *RCE. Revista de la Contratación Electrónica*, n.º 24, 2002, p. 67.

Con respecto a la importancia que comienza a cobrar el anonimato, la Recomendación n.º R (99) 5, de 23 de febrero, sobre protección a la intimidad en internet, reclama la necesidad de desarrollar técnicas que lo garanticen, al tiempo que pide confidencialidad para la información que se intercambia a través de las «autopistas de la información». La admisión del anonimato nace del respeto que merecen los derechos y las libertades de los demás y de los valores que deben ser reconocidos en una sociedad democrática.

[19] Véase CABELLO FERNÁNDEZ, M. D. ob. cit., p. 23.

[20] Recordemos que el derecho fundamental a la protección de datos ofrece dos singularidades respecto al derecho fundamental general a la intimidad personal y familiar. La primera consiste en que el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos datos que sean relevantes o tengan incidencia en el ejercicio de cualquier derecho de la persona, estén referidos o no al ámbito íntimo de la

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

derecho, y se sirve del derecho a la protección de datos para otorgar a la persona un poder de control sobre sus datos con la finalidad de impedir su tráfico ilícito y lesivo[21]. Como sabemos, el desarrollo legal del derecho fundamental a la protección de datos se realiza por medio de la LOPD[22] y del Reglamento que la desarrolla, textos en los que el referido poder de disposición y control sobre los datos personales se concreta, entre otros aspectos, en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero[23].

---

persona. El objeto de protección en este derecho no se reduce a los datos íntimos de la persona, sino que alcanza a cualquier dato que identifique o permita la identificación de la persona o que sirva para cualquier utilidad que en determinadas circunstancias constituya una amenaza para el individuo. La segunda peculiaridad radica en su contenido, pues mientras que el derecho a la intimidad personal y familiar que se consagra en el párrafo primero del artículo 18 CE otorga a la persona el poder jurídico de imponer a terceros el deber de abstenerse de realizar cualquier intromisión en su esfera íntima y la prohibición de hacer uso de lo así conocido; el derecho fundamental a la protección de datos se circunscribe a atribuir poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos referidos al modo en que deberá efectuarse el tratamiento de los datos. A este respecto véase la STC 292/2000, de 20 de julio (RTC 2000\292).

[21] En igual sentido, CABELLO FERNÁNDEZ, ob. cit., p. 5; DAVARA RODRÍGUEZ, M. Á. «Intimidad…» y LESMES SERRANO, C. *La Ley de protección de datos: análisis y comentario de su jurisprudencia*. Valladolid: Lex Nova, 2008, p. 138. DESPACHO CREMADES & CALVO SOTELO (*ob. cit.,* p. 65), aunque primeramente no diferencia entre los párrafos primero y cuarto del artículo 18 CE, sin embargo finalmente parece que también lo entiende así al dedicar un epígrafe a la aplicación de la LOPD. Antes ha mantenido que la línea doctrinal del Tribunal Constitucional que se opone al uso ilegítimo de la tecnología informática con fines de control de flujo de informaciones concernientes a cada persona resulta de aplicación también a los nuevos servicios de radionavegación o localización por satélite (GPS).

[22] La LOPD, a su vez, adaptó al ordenamiento jurídico español la Directiva 45/1996 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[23] Como se expone en la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio (RTC 1993\254), en el periodo constituyente ya preocupaba la nueva forma de amenaza concreta a la dignidad y a los derechos de la persona que surgía con la informática, siento esta la razón por la que en el párrafo cuarto del artículo 18 se encomienda al legislador (con la expresión «La ley limitará…») la tarea de establecer las garantías necesarias para proteger los derechos fundamentales que puedan resultar afectados por la expansión del tratamiento automatizado de datos. Si en un principio la inclusión en aquel tiempo de este párrafo cuarto suscitó algunas dudas relativas a su oportunidad (como quedó reflejado en el debate planteado en el Senado), singularmente por existir ya un párrafo (el primero) que procuraba en general por la protección de la intimidad de la persona, finalmente se optó por su inclusión.

Entendido de esta manera, el derecho fundamental consagrado en el artículo 18.4 CE, cuyo objetivo es limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, pasa a convertirse en un límite que no deben sobrepasar las aplicaciones que se sirvan de la geolocalización. La primera consecuencia que deriva del reconocimiento de un derecho fundamental como este es que será el usuario quien decida libremente si autoriza o no un tratamiento de sus datos de localización y, caso afirmativo, bajo qué condiciones. La aplicación que opere con geolocalización deberá garantizar al usuario del dispositivo la posibilidad de elegir la finalidad que desea otorgarle al tratamiento de sus datos de localización, además de informarle acerca de los datos concretos que serán tratados, si van a ser conocidos por terceros y el procedimiento que debe seguirse para ejercitar los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos, lo que se conoce como el «derecho a autodeterminación informativa»[24]. Es uso instaurado en la práctica que el titular de la aplicación informe sobre estos aspectos en el documento que se denomina «política de privacidad», cuya aceptación es necesaria con carácter previo a la primera utilización de la aplicación[25].

Con el párrafo cuarto se garantiza una protección específica para el caso de vulneraciones de la intimidad provenientes del uso de la informática. La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que alcanza al reconocimiento de un derecho de control sobre los datos personales. La llamada «libertad informática» debe traducirse, así, en un derecho a controlar el uso de los datos personales insertos en un programa informático («habeas data») y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (Véanse, SSTC n.º 11/1998, de 13 de enero en su Fundamento Jurídico quinto —RTC 1998\11— y n.º 94/1998, de 4 de mayo, en su Fundamento Jurídico cuarto —RTC 1998\94—).

[24] La *autodeterminación informativa* supone reconocer que debe ser la persona quien decida libremente si difunde o no sus datos personales y bajo qué condiciones. El Tribunal Constitucional, en lugar de utilizar esta expresión, prefiere utilizar como sinónima la de *libertad informática*, consagrando con ella un derecho de control sobre los datos relativos a la propia persona (*vid*. SSTC 254/1993, de 20 de julio o 292/2000, de 30 de noviembre).

[25] En la mayoría de las ocasiones el titular de la aplicación es también el responsable y encargado del tratamiento de los datos.

No obstante, esto no ocurre cuando, por ejemplo, una compañía contrata los servicios de geolocalización que ofrece otra especializada en la prestación de estos servicios. En estos casos el responsable de cualquier tratamiento indebido de datos sería la empresa que ha contratado los servicios de geolocalización, teniendo la consideración de mera encargada del tratamiento de los datos (y por lo tanto sin ser responsable fren-

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

En orden a todo lo anterior, serán las consecuencias que deriven del uso de la geolocalización las que determinen la vía concreta de protección que deba seguirse. Así, si un tratamiento indebido de los datos ha supuesto una intromisión en la vida íntima del propietario del terminal, este podrá lograr su defensa por medio del artículo 18.1 CE y, por el contrario, si el perjuicio no ha supuesto una vulneración de su intimidad, pero es consecuencia de un tratamiento indebido de datos, podrá obtener protección en virtud del artículo 18.4 CE. Una vía no excluye la otra, en el sentido de que existirán supuestos en los que lo que proceda será la aplicación concordada de los párrafos primero y cuarto del artículo 18, porque la conducta que ocasiona el perjuicio al interesado supone una vulneración de su intimidad y, al mismo tiempo, es consecuencia de un tratamiento indebido de datos (por ejemplo, se obtiene ilícitamente un patrón o perfil de conducta y se hace público en internet, sin el previo consentimiento del interesado).

III. NATURALEZA DE LOS DATOS

El dato personal es un bien jurídico protegido por el Ordenamiento Jurídico y, al mismo tiempo, susceptible de tráfico jurídico. Justamente para prevenir problemas ocasionados por el tráfico jurídico, el Derecho reconoce al titular de los datos un poder de disposición y control sobre ellos que se materializa en el derecho a consentir la recogida de los datos y a oponerse a ella y a su tratamiento; a conocer la finalidad que se le dará al tratamiento de los datos; a asegurar una recogida adecuada a la finalidad pretendida; a estar informado sobre cómo y dónde se llevará a cabo el almacenamiento y a si accederán terceros a los datos. El poder de disposición se manifiesta a través de la expresión de la voluntad del titular cuando consiente la recogida de los datos y su tratamiento o, en sentido contrario, porque la falta de consentimiento supondrá un tratamiento ilícito de datos que originará responsabilidad.

Con el propósito de lograr que cualquier tratamiento de datos respete el bien jurídico digno de protección que constituyen los datos perso-

---

te a terceros) la compañía que presta los servicios de geolocalización. A tales efectos, la LOPD diferencia entre el *responsable* del tratamiento de los datos (definido en el artículo 3.d como la persona física o jurídica que decide sobre la finalidad, contenido y uso del tratamiento) y el *encargado* del tratamiento (definido en el artículo 3.f como la persona física o jurídica que trata los datos personales por cuenta del responsable del tratamiento).

nales, el Título II de la LOPD regula en sus artículos 4 a 8 los llamados «principios de la protección de datos» (desarrollado en los artículos 8 a 12 del Título II del RLOPD)[26]. Los principios se concretan en cómo debe efectuarse la recogida de los datos personales, el valor del consentimiento del titular de los datos y el deber de información, los datos que son merecedores de una especial protección y el acceso a los datos por parte de terceros, y estos principios imponen unos deberes al responsable del tratamiento de los datos, cuyo cumplimiento contribuirá a obtener la protección debida[27].

Las aplicaciones de geolocalización deben respetar estos principios. Así, en virtud del artículo 4.1 LOPD los datos que recoja la aplicación de geolocalización para su tratamiento deberán ser exclusivamente los de localización o posicionamiento del terminal, y no otros, evitando que pueda configurarse la «trazabilidad vital» o el «patrón de conducta» de la persona. Ello es así porque en atención a que el citado artículo requiere que los datos que se recojan para su tratamiento sean *adecuados*, *pertinentes* y *no excesivos* en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Tratar los datos de localización con una finalidad distinta a la solicitada por el usuario supone una vulneración de la LOPD[28]. Los datos de posicionamiento que utilizan las aplicaciones de geolocalización son exac-

---

[26] En el entorno informático se está acuñando la expresión «privacidad desde el diseño» para aludir con ella a la observancia de estos principios ya desde el momento que se diseña el dispositivo. En concreto, consiste en la obligación de los desarrolladores y creadores de aplicaciones informáticas de introducir los principios básicos de la privacidad en el propio diseño de las aplicaciones, de forma que desde las primeras y más básicas especificaciones se vean cumplidos estos principios (véase DAVARA RODRÍGUEZ, «El tratamiento…», cit., p. 4).

[27] Coincidimos con PRATS ALBENTOSA («Segundo comentario. Principios de protección de datos: calidad de los datos, consentimiento para el tratamiento de los datos y deber de información». En *Comentario al Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (Aprobado por RD 1720/2007, de 21 de diciembre)* —Dir. Palomar Olmeda, A. y González-Espejo, P. Coord. Álvarez Rigaudias, C.—. Pamplona: Ed. Thomson Civitas, 2008, p. 159) en que, tanto el poder de disposición del titular de los datos, como los derechos de uso de quienes recogen los datos para su tratamiento, dejan escaso margen de actuación a la autonomía de la voluntad, impidiendo con ello cualquier exceso en el tratamiento de los datos por parte de la persona autorizada para ello.

[28] En el mismo sentido véase APARICIO SALOM, J. *Estudio sobre la Ley orgánica de protección de datos de carácter personal*. Cizur Menor (Navarra): Aranzadi, 2009, pp. 179-180. LESMES SERRANO (*ob. cit.*, p. 142), por su parte, indica que una recogida de datos con finalidades indeterminadas o tan vagas o genéricas que permitieran cualquier finalidad carece de validez.

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

tos por la operativa tecnológica en sí misma (basada en la triangulación de antenas, que fija la posición de cada terminal en todo momento con un pequeño margen de error) y se actualizan permanentemente, pero si a consecuencia de una transmisión deficiente los datos de localización recabados fueran incompletos, no habrían de tratarse, debiendo ser sustituidos por otros rectificados o completados a iniciativa del mismo titular de la aplicación[29].

Además, está prohibida cualquier recogida de datos de localización que se realice por medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD). Esto supone que antes de que el titular de los datos preste su consentimiento al tratamiento de los mismos tendrá que haber sido previamente informado por la aplicación de geolocalización acerca del tratamiento exacto que se hará con los datos, así como las consecuencias que tiene su prestación.

Estas consideraciones referidas a la naturaleza de los datos que trata la aplicación de geolocalización se realizan siendo conscientes de que del propietario de un terminal se tratan otros datos distintos de los de localización, en otros momentos distintos de los de ejecución de la aplicación y por otros sujetos que no son la aplicación de geolocalización (en concreto, también tratan datos el fabricante del terminal y el operador telefónico que materializa la transmisión de comunicaciones). El objeto de estudio en este trabajo son los datos de localización que emiten los terminales, no obstante y aparte de los datos de esta naturaleza, en la práctica, como decimos, se tratan otros datos personales del propietario del terminal distintos de los de localización que exigen ser mencionados, aunque solo sea para no confundirlos con los que son objeto de este estudio.

En lo que respecta al fabricante del terminal, dos son los momentos que cobran especial trascendencia en lo relativo al tratamiento de datos del usuario del dispositivo: cuando se adquiere el dispositivo y cada vez que se utiliza la geolocalización. En primer lugar, en lo que respecta al momento en que se recibe el terminal, al consistir generalmente el negocio de adquisición en una compraventa verbal, no se efectúa ninguna comunicación de datos personales por parte del adquirente del terminal.

Eso sí, como se señala en el párrafo segundo del artículo 4 LOPD, no se considerará incompatible el tratamiento posterior de estos datos con fines históricos, estadísticos o científicos.

[29] Ello sin perjuicio de la posibilidad de llegar al mismo resultado por el ejercicio del derecho de rectificación y cancelación que el artículo 16 LOPD reconoce al titular de los datos.

Solo en el caso de que durante la venta del dispositivo el fabricante requiriera la comunicación de datos personales al adquirente con la finalidad de incorporarlos a un fichero (por ejemplo, con fines comerciales), estaría obligado a informar sobre la recogida de los datos.

En segundo lugar, el fabricante del terminal puede tratar datos del usuario del dispositivo cada vez que se utiliza la aplicación de geolocalización. Aquí es necesario diferenciar dos situaciones que pueden acontecer:

a) Que el fabricante del terminal solo lo sea del hardware, no del software (esto es, el fabricante no es el titular de la aplicación de geolocalización). En estos casos, aunque el hardware propicia el inicio del tratamiento de los datos personales, ya que ofrece el posicionamiento exacto del terminal, esta transmisión de datos no debe considerarse relevante desde el punto de vista jurídico de la legislación de protección de datos, al menos en lo que atañe a exigirle obligaciones al fabricante del terminal como responsable de tratamiento de los datos, por limitarse su actuación a ser un mero prestador de acceso a servicios de telecomunicaciones o, lo que es lo mismo, un simple colaborador técnico necesario en la transmisión de los datos y cuya labor se circunscribe, no a realizar un tratamiento directo de datos, sino a posibilitar tecnológicamente que otro sujeto pueda realizarlo.
b) Que el fabricante, además de titular del hardware, sea autor o titular de la aplicación de geolocalización que se utiliza[30]. En este caso sí estará obligado a informar sobre la recogida de datos personales, ya que como titular de la aplicación es responsable del tratamiento de datos que se va a realizar.

El otro sujeto que trata datos del propietario de un terminal es la compañía telefónica que facilita la transmisión de los datos. Respecto a este operador cabe señalar que efectúa distintos tratamientos de datos, con distintas finalidades y no siempre relacionados con la ejecución de la aplicación de geolocalización, lo que obliga, a su vez, a diferenciar entre varios supuestos. La compañía telefónica recoge datos en un primer momento cuando se contrata la línea telefónica, que en el supuesto de los teléfonos móviles se identifica con la adquisición de la tarjeta

[30] Esto es lo que ocurre, por ejemplo, con los teléfonos móviles Apple, en los que esta empresa, además de fabricante del hardware del terminal, es la autora del sistema operativo (iOS) con el que opera el teléfono.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

SIM. Esta recogida de datos se diferencia de aquella otra en la que interviene la compañía telefónica cada vez que se utiliza la aplicación de geolocalización pro el tiempo en el que se realiza y por la finalidad que cumplen una y otra. El operador de telefonía recaba datos cuando se contrata la línea básicamente por dos razones, porque los necesita para el adecuado mantenimiento de la relación contractual (por ejemplo, para la facturación) y, a veces, con intención comercial (previo consentimiento informado del titular de los datos)[31]. En este caso el operador telefónico es el titular del fichero de datos que se crea, el destinatario de los datos que en él se contiene y el responsable del mismo. En el clausulado de las condiciones generales de la contratación que se incluye en el contrato de adquisición de la línea telefónica se informa de esta recogida de datos, de su inclusión en un fichero y de su posterior tratamiento[32]. En lo relativo a la finalidad comercial, y en cumplimiento del artículo 65.3 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (para la remisión de información sobre prestación

[31] Véase el artículo 48.2.b de la Ley General de Telecomunicaciones (en adelante, LGT) en relación con el artículo 15 RLOPD. De la aplicación concordada de los dos artículos se deduce que cada vez que un operador telefónico solicite durante el proceso de formación del contrato el consentimiento del titular de los datos para fines comerciales deberá permitir que el afectado pueda manifestar expresamente su negativa al tratamiento o comunicación de datos. En particular, se entiende cumplido este deber cuando se permite al interesado marcar una casilla claramente visible y que no se encuentra ya marcada.

Esta prestación de consentimiento, caso de llevarse a cabo, no es definitiva, reconociéndosele a los titulares de los datos el derecho a retirar su consentimiento para el tratamiento de los datos en cualquier momento y con efecto inmediato.

[32] Se contiene una cláusula como esta, por ejemplo, en el contrato de Telefónica Móviles España: «Telefónica Móviles España, S.A.U., en cumplimiento de la Ley Orgánica 1571999, de 13 de diciembre, de Protección de Datos de Carácter Personal, informa al cliente de que los datos personales que aporta en este acto junto con los obtenidos durante la vigencia del contrato por Telefónica Móviles España, S.A.U., o su red de distribución, serán incluidos en ficheros automatizados de datos de carácter personal titularidad de esta Empresa, responsable del tratamiento y destinataria de los datos, siendo necesarios para la relación contractual y teniendo el carácter de obligatorio a excepción de los marcados como opcionales. Asimismo, con la intención de ofrecerle nuestra mejor atención e informarle de nuestros servicios de telecomunicaciones… solicita su consentimiento para tratar, junto con los datos personales que usted nos facilita, todos los datos de tráfico necesario para realizar la facturación y pagos de las interconexiones y todos los datos de los servicios de los que sea usuario, para ofrecerle promociones comerciales[…]».

de servicios de valor añadido y sobre promociones comerciales) y del artículo 21.2 LSSI (para la remisión de publicidad comercial), el operador de telefonía está obligado a solicitar el consentimiento informado del cliente al menos con un mes de antelación al inicio de la promoción comercial o de la prestación del servicio con valor añadido[33]. Esta comunicación, que habrá de efectuarse de cualquier modo que garantice su recepción por parte del abonado, podrá materializarse de forma conjunta a la facturación del servicio prestado al abonado. Al mismo tiempo, se tendrá que facilitar al interesado un medio sencillo que no implique gasto alguno para que, si así lo desea, pueda manifestar su negativa al tratamiento de los datos[34]. Si el interesado no se pronuncia en el plazo de un mes desde que recibe la solicitud, se entenderá que consiente el tratamiento de los datos de tráfico para esta finalidad comercial, siempre que así se haya hecho constar en la información que se le remitió.

La compañía telefónica también recoge y trata datos en un segundo momento, que es cuando facilita la tarjeta SIM del terminal móvil (hoy es obligatorio entregar una fotocopia del DNI del comprador de la tarjeta o terminal móvil), así como cada vez que se establece una comunicación con el teléfono móvil (consistente en almacenar ciertos datos relativos a las comunicaciones realizadas). Estas recogidas de datos se diferencian de aquella primera por su distinta naturaleza y finalidad. Mientras que la que se realiza cuando se contrata la línea es discrecional para el operador —al menos, en lo que hace a la remisión de comunicaciones comerciales—, esta viene impuesta por la Ley 25/2007, de 18 de octubre, de conservación de datos de comunicaciones electrónicas y redes públicas de comunicación)[35]. En cuanto a su finalidad, mientras que la primera recogida venía motivada por razones de nece-

---

[33] Deberá informar del tipo de servicios para los que se efectuará el tratamiento de sus datos, los tipos de datos que serán objeto de tratamiento y la duración que tendrá.

[34] A estos efectos, es práctica extendida hacerle llegar al cliente un sobre prefranqueado o habilitar un número de teléfono gratuito.

[35] Esta ley sigue vigente, a pesar de la declaración de invalidez de la Directiva 2006/24/CE, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y de cuya transposición se ocupó. La Ley 25/2007 no ha sido derogada y, aparte de ello, el artículo 15.1 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 la privacidad y las comunicaciones electrónicas) sigue permitiendo que los Estados miembros regulen esta cuestión. En el mismo sentido, véase RODRÍGUEZ LAINZ, J. L. «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conser-

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

sidad contractual o comerciales, la segunda obedece a razones de seguridad ciudadana, como se declara expresamente en la Exposición de Motivos de la Ley 25/2007. Los datos concretos que la compañía telefónica está obligada a conservar cuando entrega la tarjeta SIM, así como los datos de cada una de las comunicaciones que se realicen desde el dispositivo móvil se enumeran en el artículo 3.1 de la Ley 25/2007[36]. Dicho lo anterior, tampoco ninguna de estas dos recogidas de datos está relacionada con el tratamiento que se realiza cuando se utiliza una aplicación de geolocalización.

Un tercer momento en el que la compañía telefónica participa en el tratamiento de datos del propietario del terminal se origina con la ejecución de la aplicación de geolocalización y consiste en la transmisión de los datos desde el terminal en el que se encuentra la señal de localiza-

---

vación de datos relativos a las comunicaciones», en *Diario La Ley*, n.º 8308, 12 de mayo de 2014.

[36] Estos datos son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación: el número de teléfono de llamada y el nombre y dirección del abonado o usuario registrado.
b) Datos necesarios para identificar el destino de una comunicación: el número o números marcados (el número o números de teléfono de destino) y los nombres y las direcciones de los abonados o usuarios registrados.
c) Datos necesarios para determinar la fecha, hora y duración de una comunicación: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
d) Datos necesarios para identificar el tipo de comunicación: el servicio telefónico utilizado, el tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) o los servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación: los números de teléfono de origen y destino; la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada; la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada; la IMSI de la parte que recibe la llamada; la IMEI de la parte que recibe la llamada.
f) Datos necesarios para identificar la localización del equipo de comunicación móvil: la etiqueta de localización (identificador de celda) al inicio de la comunicación y los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el periodo en el que se conservan los datos de las comunicaciones.

Dicho lo anterior, la ley deja claro que ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

ción hasta el gestor de la aplicación de geolocalización. La compañía telefónica actúa aquí en calidad de operador de red y como tal recibe el mismo tratamiento que los prestadores de acceso en lo relativo a la aplicación de la legislación de protección de datos. Cuando se ejecuta la aplicación de geolocalización, la compañía telefónica es un mero operador técnico necesario, limitándose su intervención a la estricta transmisión de los datos desde el terminal hasta el gestor de la aplicación de geolocalización. Esta remisión de datos que realiza el operador de telefonía es irrelevante desde el punto de vista de la legislación de protección de datos y la compañía telefónica no está obligada a informar sobre ella al usuario del dispositivo.

Dicho esto, debe mencionarse igualmente que las compañías de telefonía no contemplan el uso de la geolocalización únicamente bajo demanda del usuario del terminal, sino que en los contratos de adquisición de línea es común la inclusión de una cláusula en virtud de la cual la compañía telefónica informa al adherente de que, desde el momento de la perfección del contrato, cada vez que se marque el número de emergencias 112 se pondrá a disposición de las autoridades receptoras de estas llamadas la información relativa a la ubicación de su procedencia. El artículo 48.2.c, párrafo segundo, de la LGT preceptúa que los usuarios de los terminales no podrán rechazar el tratamiento de sus datos de localización cuando el mismo provenga de la marcación del número de emergencias 112.

Ejecutada la aplicación de geolocalización, el responsable del tratamiento está obligado a cancelar los datos de localización obtenidos a partir del terminal (art. 4.5 LOPD, en relación con el art. 8.6 RLOPD). Los datos no deberán ser conservados en forma alguna que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales han sido recabados o registrados. Tratar datos más allá del tiempo necesario o del que permita la Ley supone una infracción del artículo 6 LOPD, en tanto este tratamiento no haya sido consentido por el interesado, ni se lleve a cabo con autorización legal.

IV. EL CONSENTIMIENTO DEL TITULAR DE LOS DATOS

La regla general contenida en el artículo 6 LOPD (en relación con los arts. 10.1 y 12 RLOPD) es que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

que la ley disponga otra cosa[37]. Establecida la regla general, el mismo artículo 6 contempla algunas excepciones en su párrafo segundo, permitiendo ciertos tratamientos de datos personales sin necesidad de que el interesado haya prestado su consentimiento[38].

La actuación de la aplicación de geolocalización constituye la prestación de un servicio de la sociedad de la información y, como tal, cabe preguntarse si el tratamiento de datos que conlleva su ejecución no se corresponde con alguna de las situaciones referidas en el artículo 6.2 LOPD [en relación con el art. 10.3.B) RLOPD], en concreto, con la relativa a 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…». El tratamiento de los datos de localización es esencial para la ejecución del servicio ofrecido por la aplicación de geolocalización, ya que la falta del tratamiento impide prestar correctamente el servicio previamente solicitado por el usuario. ¿Significa esto que los tratamientos de datos que sobrevienen con el uso de las aplicaciones de geolocalización no requieren el consentimiento previo del interesado?

Coincidiendo en este punto con lo ya manifestado por Aparicio Salom, lo que debe inferirse del artículo 6.2 LOPD en cuanto a los trata-

---

[37] Por *ley* debe entenderse la LOPD o cualquier otra con rango de ley orgánica, en consideración a la reserva material que resulta de la aplicación del artículo 81 CE en relación con el 18.4 CE. Según PRATS ALBENTOSA (ob. cit., p. 178), admitir que mediante ley ordinaria puedan establecerse excepciones a este principio de la necesidad del consentimiento del interesado implicaría tanto como admitir una rebaja en el grado de tutela que exige el derecho fundamental contenido en el artículo 18.4 CE.

Sobre la importancia de la prestación del consentimiento para el tratamiento de los datos *vid*. GRIMALT SERVERA, P. en GRIMALT SERVERA, P. y CAVANILLAS MÚGICA, S. «Servicios de la sociedad de la información y protección de datos personales», en *Derecho de la empresa y protección de datos*. Ed. Thomson-Reuters Aranzadi. 2008, pp. 327 y ss.

[38] En concreto, según el artículo 6.2 LOPD, no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando 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; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

mientos de datos que son esenciales para el mantenimiento o ejecución de un contrato, no es que esos tratamientos de datos constituyan una excepción a la regla general de la exigencia del consentimiento, sino que el consentimiento ya existe desde el momento en que se perfecciona el contrato. Cuando esto ocurra deberá entenderse que el consentimiento al tratamiento de los datos se otorga junto al prestado para la perfección del contrato[39]. Dentro de los contratos en los que el tratamiento de datos es esencial para su correcto desarrollo debe diferenciarse entre los contratos en los que el tratamiento de datos es necesario para su mantenimiento y ejecución (p. ej., contratos de tracto sucesivo, de suministro, bancarios, etc.), y aquellos otros en los que el tratamiento de datos es el objeto del contrato, siendo necesario el consentimiento del interesado para el tratamiento de los datos, tanto para unos, como para otros. No obstante, mientras que los contratos en los que el consentimiento para el tratamiento de los datos es necesario para su mantenimiento y ejecución el consentimiento prestado para el contrato principal se entiende prestado también para el tratamiento de los datos (lo que permite el artículo 6.2 LOPD); en los segundos, teniendo en cuenta que el tratamiento de los datos constituye el objeto de los mismos, el consentimiento deberá otorgarse de forma expresa o bien deducirse de actuaciones del interesado. Por pertenecer las aplicaciones de geolocalización a este segundo grupo de relaciones contractuales, el tratamiento de los datos de localización que en ellas se realiza requiere que se preste un consentimiento inequívoco por parte del interesado.

En cuanto a los menores, podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en los casos en los que la ley exija la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores (art. 13.1 RLOPD). La capacidad exigida para prestar el consentimiento al tratamiento de los datos no debe confundirse con la requerida para la adquisición de un terminal o la contratación de la aplicación de geolocalización, que es la general para obligarse (art. 1263 CC). Si un menor de edad mayor de catorce años adquiere un terminal móvil, el contrato será anulable (salvo que se demuestre que la compraventa se realiza con el consentimiento de sus padres, que será válido), pero el consentimiento que haya prestado para el tratamiento de los datos podrá considerarse válido.

Respecto a la solicitud de consentimiento, deberá ir referida a vincular los datos de posicionamiento del terminal con la específica finali-

[39] APARICIO SALOM, ob. cit., pp. 140-141.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

dad que se pretenda con la aplicación, delimitando las condiciones especiales que, de existir, concurran en el tratamiento (p. ej., si los datos van a quedar almacenados durante cierto tiempo o si se van a ceder a algún tercero). La prueba de la existencia del consentimiento del titular de los datos recae sobre el responsable del tratamiento, que es el titular de la aplicación de geolocalización (art. 12.3 RLOPD)[40].

La necesaria prestación de consentimiento del usuario implica que cualquier aplicación de geolocalización deberá estar desactivada por defecto cuando se adquiera el terminal[41]. En atención a los riesgos ya mencionados que el uso de la geolocalización presenta para la intimidad de las personas, sería deseable que el responsable de la aplicación de geolocalización informara sobre ello a los usuarios antes de utilizar la aplicación por primera vez[42]. En este sentido, dos buenas medidas que podrían adoptarse serían, por una parte, limitar temporalmente el alcance de la prestación de consentimiento, obligando al propietario del terminal a renovarlo periódicamente y, por otra parte, que la misma aplicación de geolocalización advirtiera de su activación con un icono permanentemente visible en el dispositivo cada vez que esté operando[43].

En lo que respecta al tiempo en que debe obtenerse el consentimiento, deberá recabarse antes de utilizar la aplicación por primera vez (art. 16 RLOPD en relación con el art. 48.2.c LGT), por originarse ya en ese momento el primer tratamiento de datos.

En la prestación de consentimiento rige el principio de libertad de forma (art. 14 RLOPD), por no ser los datos de geolocalización ninguno de los especialmente protegidos que requieren un consentimiento

---

[40] Véanse SSAN, Sección 1.ª, de 25 de octubre de 2002 (JUR 2003\25510) y 30 de junio de 2004 (RJCA 2004\669).

[41] Así lo aconseja en sus conclusiones el Dictamen del Grupo de Trabajo del artículo 29, el 16 de mayo de 2011, referido a los servicios de geolocalización en los teléfonos móviles (págs. 15 y 20), cuando dice que los servicios de localización deben estar apagados y que la activación de estos servicios requiere de un consentimiento informado y específico a los diferentes fines para que los datos sean captados o almacenados.

[42] Siguiendo en este punto la directriz III.2 de la Recomendación n.º R(99)5 del Comité de Ministros de los Estados miembros sobre la protección de la intimidad en internet, en el que se contienen las Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información" (adoptada por el Comité de Ministros el 23 de febrero de 1999, durante la 660.ª reunión de Delegados de Ministros).

[43] Véase Dictamen del Grupo de Trabajo del artículo 29, el 16 de mayo de 2011, referido a los servicios de geolocalización en los teléfonos móviles, p. 15.

expreso[44]; o expreso y, además, por escrito[45]. Lo único que se exige es que el consentimiento sea *inequívoco*, entendiéndose por tal aquel cuya prestación no deja lugar a dudas. Así, será válida, tanto una prestación de consentimiento expresa (p. ej. la activación de una casilla habilitada específicamente para ello que aparezca en la pantalla del terminal)[46], como una prestación de consentimiento tácita que no deje lugar a dudas sobre su otorgamiento (p. ej., la ejecución directa de la aplicación de geolocalización, habiendo pasado previamente por una pantalla en la que se informa acerca de la necesidad del consentimiento y su finalidad)[47].

El hecho de que en la práctica estas dos modalidades sean las más extendidas no significa que otros medios de prestar el consentimiento, como el envío de un correo electrónico, no sean válidos. En este sentido, el legislador describe en el artículo 14 RLOPD, a modo de ejemplo, un procedimiento que puede seguirse por parte del responsable del tratamiento para recabar el consentimiento del titular de los datos, quedando a su libertad utilizarlo o seguir otro[48]. El silencio del interesado no acompañado de ningún otro acto que inequívocamente pueda interpre-

---

[44] Datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual (art. 7.3 LOPD).

[45] Datos de carácter personal que revelen ideología, afiliación sindical, religión y creencias (art. 7.2 LOPD).

[46] En virtud de los artículos 1262.3 CC y 22.2 LSSI, se admite la prestación de consentimiento a través del propio terminal. En el artículo 22.2 LSSI se establece que, cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.

[47] Véase APARICIO SALOM, ob. cit., p. 135 o LESMES SERRANO, ob. cit., p. 193. Eso sí, como apunta ECIJA ABOGADOS (*Factbook Protección de datos personales: el manual práctico para cumplir la Ley y el Reglamento LOPD*. Cizur Menor: Thomson Aranzadi, 2008, p. 60), para que pueda considerarse que el consentimiento tácito ha sido recabado lícita y adecuadamente se exige haber cumplido el deber de información que impone el artículo 5 LOPD.

[48] El procedimiento que se propone en este artículo parte de que el responsable del tratamiento se dirija al titular de los datos, informándole en los términos previstos en los artículos 5 LOPD y 12.2 RLOPD y concediéndole un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse se entenderá que consiente el tratamiento de sus datos de carácter personal.

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

De igual forma, deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará válido que tal negativa pueda efectuarse mediante un envío prefranqueado o la llamada a un

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

tarse como manifestación de voluntad favorable al tratamiento de los datos no podrá presumirse como prestación de consentimiento[49]. En sede de geolocalización no cabe aplicar el artículo 14.2 LOPD, en el que se contempla la posibilidad de que el silencio continuado durante treinta días por parte del interesado se entienda como favorable al tratamiento de sus datos personales, porque en el supuesto regulado en este artículo se parte de que el responsable del tratamiento ya dispone de los datos del interesado que desea tratar cuando solicita su consentimiento. La aplicación de este artículo no procede, además, porque los datos que serán objeto de tratamiento se generan a partir de la ejecución de la aplicación, lo que en sí mismo debe interpretarse como una prestación tácita de consentimiento, válida si el titular de los datos fue debidamente informado previamente a ejecutar la aplicación.

El tratamiento de datos de posicionamiento sin el consentimiento de su titular se considera infracción grave (art. 44.3.b LOPD)[50], salvo en aquellos casos en los que la ley le otorgue otra calificación, y lleva aparejado una sanción de multa de 40.001 a 300.000 euros (art. 45.2 LOPD). La imposición de dicha multa no priva al interesado de poder solicitar una indemnización por los daños y perjuicios que el tratamiento de los datos pudiera haberle acarreado (art. 19.1 LOPD, en relación con el art. 1101 CC).

---

número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

Termina aclarando que, cuando se solicite el consentimiento del interesado a través del procedimiento descrito en el artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

[49] Véase en este sentido la STS de 19 de diciembre de 1990 (RJA 10287), en la que se aclara que el mero silencio (no acompañado de ningún otro acto) no es productor de efectos jurídicos más que en el caso de que la ley o la voluntad de las partes así se lo haya reconocido previamente, pudiendo hablarse de un silencio cualificado solo cuando se acompañe de hechos positivos precedentes, a una actividad anterior de la parte que guardó silencio o a particulares situaciones subjetivas u objetivas que sirvan como elemento útil para tener por hecha la manifestación de una determinada voluntad. No es este el caso en el que se encuentra la geolocalización. Véanse también: SSTS de 24 de noviembre de 1943 (RJA 1943\1292), de 24 de enero de 1957 (RJA 1957\367), de 30 de noviembre de 1957 (RJA 3570), de 9 de noviembre de 1959 (RJA 1959\4924), de 25 de enero de 1961 (RJA 1961\285), de 3 de febrero de 1962 (RJA 1962\648), de 27 de enero de 1964 (RJA 1964\388), de 29 de enero de 1965 (RJA1965\262), de 10 de junio de 1966 (RJA 1966\3028).

[50] La Resolución de la Agencia Española de Protección de Datos por la que se imponga la sanción en los supuestos de tratamiento ilícito de datos agota la vía administrativa (art. 48.2 LOPD).

Como complemento a la prestación de consentimiento, el titular de los datos debe recibir del responsable del tratamiento (el titular de la aplicación) *previamente* a la recogida de los datos y de modo *expreso*, *preciso* e *inequívoco* cierta información que se detalla en el artículo 5 LOPD. En concreto, deberá ser informado sobre: a) la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información; b) el carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas (esto resulta aplicable en geolocalización para aquellas situaciones en las que se recaben otros datos aparte de los de posicionamiento —p. ej., personales del propietario del terminal—); c) las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Expuesto lo anterior, en sede de geolocalización el titular de la aplicación, como responsable del tratamiento de los datos, no estará obligado a informar sobre el contenido de la letra c), por deducirse claramente de las circunstancias que su negativa al acceso de los datos de posicionamiento supondrá la imposibilidad de ejecución de la aplicación (art. 5.3 LOPD)[51]. La entrega de esta información ayuda a obtener un consentimiento informado por parte del titular de los datos y evita la existencia de vicios del consentimiento como, por ejemplo, el del error, tanto en la prestación en sí, como en su alcance o contenido[52].

El término *previamente* debe interpretarse en el sentido de que el propietario del terminal sea informado sobre la procedencia de la reco-

---

[51] El artículo 5.3 LOPD también contempla la posibilidad de no informar sobre el contenido de las letras b) (carácter obligatorio o facultativo de la respuesta a la recogida de los datos y de los destinatarios de la información), ni d) (la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición), cuando ello también sea deducible de la naturaleza de los datos que se solicitan o de las circunstancias en que se recaban. Sin embargo, a diferencia de lo que ocurre para la letra c), estimamos que aquí no procede la exención de informar, por no ser ninguno de estos dos contenidos deducibles de los datos que se solicitan, ni de las circunstancias en que se recaban los datos.

[52] No en vano, en la Recomendación 1/99 del Grupo de Trabajo del artículo 29, sobre el tratamiento invisible y automático de datos personales en internet efectuado por software y hardware, aprobada el 23 de febrero de 1999 (5093/98/ES/final WP 17), se alude a la preocupación que suponen los tratamientos de datos de personas que desconocen por completo tal tratamiento. En la Recomendación se insta a los titulares de *software* y *hardware* a tomar en consideración y respetar los principios de la protección de datos, en especial el de informar acerca del mismo, con el fin de que siempre pueda darse un consentimiento informado.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

gida de los datos y del resto de aspectos contenidos en el artículo 5 LOPD durante el proceso de instalación de la aplicación en el terminal (lo que ocurrirá cada vez que haya sido necesario instalar la aplicación con posterioridad a la adquisición del terminal) o, cuanto menos, con anterioridad a la primera ejecución de la aplicación (para aquellos casos en los que la aplicación de geolocalización venga instalada por defecto en el terminal, conformando parte de su software).

Para que al propietario del terminal no le quede duda alguna en cuanto al alcance que tiene el consentimiento que presta, y a que los datos referentes a su ubicación serán utilizados por la aplicación de geolocalización cada vez que la ejecute, el titular de la aplicación deberá facilitar esa información de forma *expresa*, *precisa* e *inequívocamente*. La ausencia de la mencionada información o un mero aviso consistente en informarle de que la aplicación se servirá de los datos de ubicación del terminal contenido dentro de otro aviso más general en el que se alude a cuestiones técnicas (como las características del programa, el espacio que ocupa o los requerimientos mínimos informáticos que requiere para poder operar) debe considerarse un incumplimiento del deber de informar[53]. Un aviso como este no puede considerarse válido, en tanto no cumple ninguno de los tres requisitos que se exigen en el artículo 5 LOPD: adolece de precisión jurídica (no se informa en sentido jurídico, sino meramente técnico), no es expreso (no se solicita explícitamente el consentimiento del titular, ni se indican las consecuencias jurídicas que tiene la recolección de los datos) y se presta a equívocos (el titular de los datos puede pensar que está recibiendo una mera información técnica).

A semejanza de lo que ocurría con la prestación de consentimiento por medio del propio dispositivo, en la actualidad es frecuente que el titular de la aplicación facilite al usuario la información a través del mismo terminal y, para asegurarse la prueba del cumplimiento de esta obligación, la propia aplicación de geolocalización impide que el usuario preste el consentimiento sin haber recibido antes la información, e impida que utilice la aplicación sin haber prestado antes el consentimiento[54].

---

[53] Estos avisos generales se generan en la mayoría de las ocasiones, no por la aplicación de geolocalización, sino directamente por el software del terminal y vienen a constatar que la aplicación de geolocalización cumple los requisitos técnicos exigidos por el software del terminal para poder ejecutarse.

[54] La AEPD señala en su Informe Jurídico 93/2008, relativo a las formas de obtener el consentimiento mediante web: consentimientos tácitos, que «en cuanto al consentimiento informado, este habrá de recabarse de tal forma que resulte imposible la

El incumplimiento de este deber de informar por parte del titular de la aplicación se considera infracción leve (art. 44.2.c LOPD) y lleva aparejada una sanción de multa de 900 a 40.000 euros (art. 45.1 LOPD). A semejanza de lo que ocurre cuando se tratan datos sin el consentimiento del interesado, la imposición de la multa no priva al interesado de poder solicitar además una indemnización por los daños y perjuicios que dicho tratamiento pudiera haberle ocasionado.

V. EL EJERCICIO DE DERECHOS POR EL INTERESADO

Consecuencia de que los datos de posicionamiento del terminal de un usuario sean tratados por la aplicación de geolocalización, el titular de los mismos podrá ejercitar los derechos de acceso, rectificación, oposición o cancelación que se reconocen en los artículos 15 a 17 LOPD, en relación con los artículos 27 a 36 RLOPD. Por el derecho de acceso (art. 15 LOPD, en relación con arts. 27 a 30 RLOPD) el titular de los datos podrá solicitar y obtener información relativa a qué datos personales suyos han sido objeto de tratamiento, a cómo se han obtenido y a todo lo referente a las comunicaciones que se quieren hacer con ellos.

El titular de la aplicación de geolocalización está obligado a resolver sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud (art. 29 RLOPD). Transcurrido el plazo sin que de forma expresa el titular de la aplicación de geolocalización responda a la petición de acceso, el interesado podrá reclamar ante la AEPD, según se establece en el artículo 18 LOPD[55]. El titular de la aplicación de geolocalización podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

---

introducción de dato alguno sin que previamente el interesado haya conocido la advertencia que contenga las menciones a las que nos hemos referido (alude con ello a los derechos que se le reconocen a todo titular de datos), pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho referencia. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco tal y como exige la Ley».

[55] O la Agencia Vasca de Protección de Datos o la Autoridad Catalana de Protección de Datos, que conocerán de los asuntos que afecten a ficheros cuya titularidad la ostenten órganos de su respectiva Administración autonómica o local.

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

Mediante el ejercicio de los derechos de rectificación y cancelación (art. 16 LOPD, en relación con arts. 31 a 33 RLOPD) se solicita al titular de la aplicación de geolocalización la rectificación de los datos que está tratando (p. ej., piénsese en el caso de que el interesado ha prestado su consentimiento con el propósito de que los datos se utilicen para una determinada finalidad y, sin embargo, el titular de la aplicación los usa para otra) o su cancelación (p. ej., porque el interesado no desea que se sigan tratando sus datos de posicionamiento). Las solicitudes de rectificación deberán indicar los datos concretos a que se refieren.

El titular de la aplicación de geolocalización está obligado a resolver sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer una reclamación ante la AEPD. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el titular de la aplicación de geolocalización deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que este, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda asimismo a rectificar o cancelar los datos.

Al ejercitar el derecho de oposición (art. 17 LOPD, en relación con arts. 34 a 36 RLOPD), el titular de los datos muestra su oposición a que estos sean tratados. El ejercicio del derecho de oposición en el ámbito de las aplicaciones de geolocalización será muy residual, ya que este derecho se configura fundamentalmente para ejercitarlo en casos en los que no es necesario recabar el consentimiento del interesado para el tratamiento de sus datos. Este supuesto no se produce cuando se utilizan aplicaciones de geolocalización, en las que, como se ha visto, la prestación del consentimiento es requisito necesario para el tratamiento de los datos de posicionamiento. Tendrá sentido el ejercicio de este derecho, por ejemplo, cuando se estén tratando datos de posicionamiento a consecuencia de que la aplicación de geolocalización estuviera activada en el terminal de forma predeterminada.

El titular de la aplicación de geolocalización deberá resolver sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer reclamación ante la AEPD.

A fin de que los usuarios de las aplicaciones de geolocalización puedan ejercitar correctamente estos derechos, el titular de la aplicación de geolocalización debe facilitar al interesado un medio sencillo y gratuito para el ejercicio de estos derechos (art. 24.2 RLOPD). Los dere-

chos de acceso, rectificación, cancelación y oposición son derechos independientes, lo que supone que el ejercicio de cualquiera de ellos no está condicionado al ejercicio previo de ninguno de los otros[56].

Si el ejercicio de los derechos frente al titular de la aplicación fuera infructuoso, el interesado puede denunciar la situación ante la Agencia Española de Protección de Datos o acudir a los tribunales de justicia, sin que, como se verá inmediatamente después, el seguimiento de una de estas vías excluya la otra. Si el camino elegido por el interesado es denunciar la situación ante la AEPD, vía esta seguida en la práctica por la mayoría de los afectados que denuncian un tratamiento indebido de datos, la AEPD estudiará la procedencia o improcedencia de la denegación[57]. Contra las resoluciones de la AEPD procederá, bien recurso de

---

[56] El procedimiento a seguir en el ejercicio de estos derechos se regula en los artículos 24 a 26 RLOPD. Si la aplicación de geolocalización dispone de un servicio de atención al cliente, el interesado podrá ejercitar estos derechos a través de dicho servicio.

Cuando el ejercicio de cualquiera de estos derechos no se realice por medio del servicio de atención al cliente, sino por escrito dirigido al titular de la aplicación de geolocalización, deberá incluirse:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación.
   Es posible también utilizar firma electrónica. En este caso, el uso de la firma electrónica identificativa del interesado eximirá de la presentación de las fotocopias del DNI o documento equivalente.
b) Petición en que se concreta la solicitud.
c) Dirección a efectos de notificaciones, fecha y firma del solicitante.
d) Si se tuvieran, documentos acreditativos de la petición que formula.

En el caso de que a la solicitud le falte alguno de estos contenidos, el titular de la aplicación de geolocalización deberá solicitar su subsanación.

El titular de la aplicación de geolocalización deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el interesado aun cuando este no haya utilizado el procedimiento que se haya establecido específicamente para ello, siempre que se haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que esta contenga la información que se solicita.

[57] Recibida la reclamación, la AEPD dará traslado de la misma al titular de la aplicación de geolocalización, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes. Recibidas las alegaciones o transcurrido el plazo previsto sin recibir contestación, la AEPD resolverá sobre la reclamación formulada (previa recopilación de los informes, pruebas y otros actos de instrucción que estime pertinentes, incluida la audiencia del interesado y nuevamente la del responsable del fichero). Véanse artículos 117 y ss. RLOPD.

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

reposición ante el Director de la Agencia, bien directamente recurso contencioso-administrativo.

VI. RÉGIMEN DE RESPONSABILIDAD

Si bien en un principio la respuesta a la pregunta de quién debe responder por los tratamientos indebidos o deficientes de datos que acontezcan con el uso de una aplicación de geolocalización puede parecer fácil, en el sentido de que debe serlo el responsable del tratamiento, la realidad demuestra que es bastante más complicado de lo que parece, aunque solo sea por la pluralidad de sujetos que, como se ha visto cuando se analizó la naturaleza de los datos, intervienen en la transmisión de esos datos[58].

Partiendo de la regla de que cada sujeto será responsable de su propia actuación y de que será la calidad de su intervención en la transmisión de los datos la que determine el alcance de su responsabilidad[59], la delimitación del régimen de responsabilidad ante tratamientos indebidos o defectuosos de datos en la geolocalización pasa necesariamente por realizar un análisis diferenciado de las dos situaciones que pueden plantearse, en función de que el fabricante del dispositivo sea al mismo tiempo autor/titular de la aplicación de geolocalización o no lo sea.

a) Si el fabricante del dispositivo, además de fabricante del hardware, es autor de la aplicación de geolocalización (o esta viene preinstalada por defecto en el terminal) será responsable de cualquier tratamiento indebido o deficiente de datos que se rea-

---

El plazo máximo del que dispone la AEPD para dictar y notificar resolución es de seis meses, a contar desde la fecha de recepción de la reclamación del interesado. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, la reclamación se considerará estimada por silencio administrativo positivo.

Si la resolución de tutela fuese estimatoria se requerirá al titular de la aplicación de geolocalización para que, en el plazo de los diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la AEPD en idéntico plazo.

[58] Con la expresión *tratamiento indebido* se alude al tratamiento de datos sin consentimiento del titular o para una finalidad distinta de la autorizada por el titular de los datos. Con la de *tratamiento deficiente*, a aquel tratamiento de datos realizado con consentimiento del titular, pero con datos obsoletos.

[59] La geolocalización es un servicio de la sociedad de la información y como tal reproduce algunos de los problemas generales característicos de este sector, siendo una prueba evidente de ello este de la delimitación del régimen de responsabilidad.

lice con la aplicación. En esta hipótesis es preciso tener en cuenta que existen fabricantes de teléfonos móviles que, aun no siendo autores del software que llevan incorporado sus dispositivos, lo distribuyen bajo una licencia de explotación concedida por su autor (como ocurre en la práctica generalidad de los casos en los que la aplicación viene preinstalada por defecto)[60]. En cualquiera de estos supuestos el fabricante del teléfono será responsable del tratamiento de datos que se origina con la aplicación de geolocalización. Este mismo criterio debe aplicarse en el supuesto de los navegadores de los automóviles.

Cabría preguntarse si en estas situaciones es posible exigir responsabilidad al operador de la red de telecomunicaciones por la que se transmiten los datos (el operador de telefonía o de redes wifi). La figura del operador de red se recoge en el artículo 14 LSSI entre los prestadores de servicios de intermediación en la sociedad de la información, indicándose en el citado precepto que estos prestadores de servicios de intermediación no serán responsables de los hechos generadores de responsabilidad que nazcan de los contenidos de datos que se transmiten por las redes de comunicaciones de las que son titulares. El único caso en el que deberán responder es cuando ellos mismos hayan originado la transmisión, modificado los datos o seleccionado estos o a los destinatarios de dichos datos, y ninguna de estas situaciones acontece en el supuesto de las aplicaciones de geolocalización[61]. La posición que adopta el legislador en la LSSI respecto a los operadores de redes de telecomunicación es razonable, al limitarse su intervención a ofrecer los medios téc-

[60] En esta situación se pueden encontrar, por ejemplo, teléfonos de empresas como Samsung, Sony o LG, cuyo software (Android), habiendo sido desarrollado por Google, sin embargo es distribuido por ellas en virtud de licencia.

[61] En concreto, según el artículo 14 LSSI, «los operadores de redes de telecomunicaciones y proveedores de acceso a una red de telecomunicaciones que 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 tiene lugar durante su transmisión. Las actividades de transmisión y provisión de acceso a que se refiere el apartado anterior 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».

Derecho Privado y Constitución
ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

nicos necesarios (soportes materiales, conexiones, etc.) para que otros sujetos puedan prestar servicios de la sociedad de la información (los titulares de las aplicaciones de geolocalización), sin que su participación tenga incidencia material directa en la ejecución del servicio concreto que se presta. Dicho con otras palabras, el proveedor de red es un operador tecnológicamente necesario en la prestación de cualquier servicio de la sociedad de la información, sin que su actuación llegue más allá de la puesta a disposición material de la red de comunicaciones necesaria para prestar el servicio[62].

b) Por el contrario, si el fabricante del dispositivo no es el autor de la aplicación de geolocalización con la que opera el dispositivo, ni esta venía preinstalada por defecto en el terminal (p. ej., piénsese en todos aquellos supuestos en los que ha sido el propio usuario quien ha descargado la aplicación de geolocalización de internet), no responderá de los tratamientos indebidos o deficientes de datos, debiendo hacerlo el titular de la aplicación de geolocalización (art. 43 LOPD). En estos casos responde el titular de la aplicación de geolocalización por ser él el responsable del tratamiento de los datos. La responsabilidad que aquí dimana del artículo 43 LOPD debe ser puesta en relación con la que, de un modo más general, se establece en el artículo 13 LSSI para todos los prestadores de servicios de la sociedad de la información. Según este artículo, los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico (donde debe incluirse la derivada del incumplimiento de la normativa de protección de datos) y «sin perjuicio de lo que se dispone en la LSSI»[63]. En el caso

[62] Si el operador de red de telecomunicación no se limitara a poner la red de telecomunicaciones a disposición de los usuarios, sino que, además de ello, desempeñara alguna otra labor con los datos (por ejemplo, los tratara para su correcta transmisión o hiciera copias temporales de los mismos), entonces sí cabría exigirle responsabilidad en la medida establecida en los artículos 14 a 17 de la LSSI, que regulan la responsabilidad de los prestadores de servicios de intermediación. En estos casos, el operador de la red de telecomunicación, en cumplimiento del artículo 11 LSSI, está sujeto a un deber de colaboración consistente en suspender la labor que está realizando cuando le sea ordenado por el órgano competente. La infracción de este deber se califica como «muy grave» en el artículo 38.2.b LSSI.

[63] El legislador se refiere con este último inciso a la responsabilidad en la que pueden incurrir los diferentes prestadores de servicios de *intermediación* mencionados

> que estamos tratando el fabricante del terminal está exento de responsabilidad porque su intervención se limita a ser un operador técnico necesario para que sea posible realizar la comunicación (la antena contenida en el terminal será la que indique a la aplicación de geolocalización la ubicación), pero no realiza ningún tratamiento de datos.

En cuanto a la responsabilidad del operador de la red de telecomunicaciones en este caso, se aplicará el mismo razonamiento que se expuso al analizar la situación A).

Teniendo en cuenta que el artículo 19 LOPD reconoce la posibilidad a los interesados de ser indemnizados por los daños o lesiones en sus bienes que se hayan ocasionado a consecuencia de un tratamiento indebido de datos, dichos titulares, aparte de denunciar el tratamiento indebido de datos originado en la aplicación de geolocalización ante la AEPD, lo que dará lugar a la imposición por parte de esta al responsable del tratamiento de sanciones si finalmente se prueba que el tratamiento de datos ha sido indebido, siempre podrán recabar de los órganos de la jurisdicción ordinaria la tutela de sus derechos (salvo, claro está, que se trate de ficheros de titularidad pública, en cuyo caso la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas)[64]. Esto último ocurrirá, bien cuando el interesado acuda directamente a los tribunales de justicia (sin haberse dirigido previamente a la AEPD, pues no está obligado a ello), bien cuando, habiéndose dirigido a la AEPD (procedimiento que, como se ha apuntado, puede concluir con la imposición de una sanción económica para el responsable del tratamiento), además reclama una indemnización por los daños que el tratamiento indebido le ha ocasionado. Obsérvese que la diversa naturaleza de las vulneraciones de derechos puede dar como resultado en ocasiones no solo la imposición de sanciones administrativas al responsable del tratamiento, sino que también pueden ser originadoras de responsabilidad civil, como podría ocurrir, por ejemplo, en el supuesto en que los datos

---

en la LSSI: operadores de redes y proveedores de acceso; prestadores de servicios que realizan copia temporal de los datos solicitados a los usuarios; prestadores de servicios de alojamiento o almacenamiento de datos; y, por último, prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.

[64] Sobre esta cuestión véase GÓMEZ MARTÍNEZ, C. «El ejercicio de acciones civiles de protección de la intimidad del usuario de internet. Aspectos procesales», *Derecho a la intimidad y nuevas tecnologías*. Madrid: Ed. Consejo General del Poder Judicial, 2004, p. 153.

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02

de posicionamiento de un terminal son utilizados por la aplicación de geolocalización sin el consentimiento del titular de los datos para remitir mensajes publicitarios de establecimientos comerciales próximos al lugar de ubicación del terminal (en suma, para una finalidad no autorizada por el titular)[65].

BIBLIOGRAFÍA

APARICIO SALOM, J. (2009): *Estudio sobre la Ley orgánica de protección de datos de carácter personal*, Cizur Minor (Navarra), Ed. Aranzadi.

BARINAS UBIÑAS, D. (2013): «El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada», en *Revista Electrónica de Ciencia Penal y Criminología*, 15-09, pp. 09:1-09:60.

CABELLO FERNÁNDEZ, M. D. (2011): «Protección de datos e internet», *RCE. Revista de la Contratación Electrónica*, n.º 116, noviembre-diciembre, pp. 3-24.

CAMPUZANO TOMÉ, H. (2000): *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*, Madrid, Ed. Tecnos.

DAVARA RODRÍGUEZ, M. Á. (2013): «El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho», en *Diario La Ley*, n.º 8157, 26 de septiembre de 2013, pp. 1-8.

— (2009) «Intimidad, protección de datos y seguridad: un difícil equilibrio», en *Diario La Ley*, n.º 7276, 4 de noviembre de 2009.

DESPACHO CREMADES & CALVO SOTELO (2002): «Estatuto jurídico de los servicios de radiolocalización (GPS) a través de redes de telefonía móvil (GSM), *RCE. Revista de la Contratación Electrónica*, n.º 24, pp. 47-76.

ÉCIJA ABOGADOS (2008): *Factbook Protección de datos personales: el manual práctico para cumplir la Ley y el Reglamento LOPD*, Cizur Menor (Navarra), Ed. Thomson Aranzadi.

GIL ANTÓN, A. M.: «La privacidad del menor en internet», en *REDS* n.º 3, septiembre-diciembre 2013.

GÓMEZ MARTÍNEZ, C. (2004): «El ejercicio de acciones civiles de protección de la intimidad del usuario de internet. Aspectos procesales», *Derecho a la intimidad y nuevas tecnologías*, Madrid, Ed. Consejo General del Poder Judicial.

[65] En este punto atiéndase a que el artículo 30 LSSI recoge la llamada «acción de cesación», que se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la LSSI, cuando dicha conducta lesione intereses colectivos o difusos de los consumidores. Junto a esta acción, en el párrafo segundo reconoce la llamada «acción de prohibición», cuyo ejercicio busca evitar que pueda repetirse en el futuro un comportamiento que se ha producido en el pasado y del que existen indicios que llevan a pensar que puede volver a suceder.

GRIMALT SERVERA, P.: «Los menores e internet: capacidad *versus* protección de la vida privada», en *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa* (coords. Cuena Casas, Anguita Villanueva, Ortega Doménech), Madrid, Ed. Dykinson, 2013.

GRIMALT SERVERA, P. y CAVANILLAS MÚGICA, S.: «Servicios de la sociedad de la información y protección de datos personales», en *Derecho de la empresa y protección de datos*. Ed. Thomson-Reuters Aranzadi. 2008.

LESMES SERRANO, C. (2008): *La Ley de protección de datos: análisis y comentario de su jurisprudencia*, Valladolid, Ed. Lex Nova.

MEGÍAS TEROL, J.: «Privacy by design, construcción de redes sociales garantes de la privacidad», en *Derecho y redes sociales* (editores Rallo Lombarte y Martínez Martínez). Segunda edición. Ed. Civitas Thomson Reuters, 2013.

OROZCO PARDO, G.: «Intimidad, privacidad, «eximidad», y protección de datos del menor. ¿Un cambio de paradigma?», en *La protección jurídica de la intimidad* (Coords. Javier Boix Reig, Ángeles Jareño Leal), Ed. Iustel, Madrid, 2010;

PANIZA FULLANA, A.: «Problemática jurídica del menor como consumidor/usuario en la sociedad de la información», en *Congreso Derecho y Nuevas Tecnologías*, Universidad de Deusto, Bilbao, 2009.

PÉREZ LUÑO, A. E.: «La protección de los datos personales del menor en internet», en *Anuario Facultad de Derecho de la Universidad de Alcalá*, 2009.

PIÑAR MAÑAS, J. L.; «El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales», en *Redes sociales y privacidad del menor*. Editorial Reus, 2011.

PRATS ALBENTOSA, L. (2008): «Segundo comentario. Principios de protección de datos: calidad de los datos, consentimiento para el tratamiento de los datos y deber de información». En *Comentario al Reglamento de desarrollo de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (Aprobado por RD 1720/2007, de 21 de diciembre)*, (Dir. Palomar Olmeda, A. y González-Espejo, P. Coord. Álvarez Rigaudias, C.), Pamplona, Ed. Thomson Civitas, pp. 157-212.

RODRÍGUEZ LAINZ, J. L. (2012): «Los dispositivos electrónicos de posicionamiento global (GPS) en el proceso penal», *Diario La Ley*, n.º 7945, de 17 de octubre de 2012, pp.1-8.

— (2014): «Sobre la incidencia de la declaración de invalidez de la Directiva 2006/24/CE en la ley española sobre conservación de datos relativos a las comunicaciones», en *Diario La Ley*, n.º 8308, 12 de mayo de 2014, pp. 1-10.

VELASCO NÚÑEZ, E. (2014): «Tecnovigilancia, geolocalización y datos: aspectos procesales penales». En *Diario La Ley*, n.º 8338, Sección Doctrina, 23 de junio de 2014, pp. 1-9.

ISSN-L: 1133-8768. Núm. 29, enero-diciembre 2015. Págs. 47-82
http://dx.doi.org/10.18042/cepc/dpc.29.02