Grado en Derecho

Facultad de Derecho

Universidad de La Laguna

Curso 2016/ 2017

Convocatoria: Septiembre

LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD EN RELACIÓN A LA GEOLOCALIZACIÓN

THE DATA PROTECTION AND PRIVACY RIGHTS RELATED TO GEOLOCATION

Realizado por la alumna Dª Natalia Hernández Delgado.

Tutorizado por la Profesora Dª Estefanía Hernández Torres.

Departamento: Disciplinas Jurídicas Básicas.

Área de conocimiento: Derecho Civil.

ABSTRACT

Our personal data contains a large amount of information about us and among these it is found the location data, which is why our work focuses on analyzing the data processing and how it is tied with privacy and rights related to the personality.

In addition, our objective is to highlight the risks associated with the use of the geolocation along with the review of the rights that the users own and the obligations and duties that must be respected by those who handle these location data to which we will refer in this study.

WORD KEYS: geolocation, privacy and rights related to the personality, data protection.

RESUMEN

Nuestros datos personales contienen gran cantidad de información sobre nosotros y, entre estos, se encuentran los datos de ubicación. Es por ello que nuestro trabajo se centra en analizar el tratamiento de datos y su relación con los derechos de la personalidad.

Asimismo, nuestro objetivo es poner de manifiesto los riesgos que conlleva el uso de la geolocalización junto con el análisis de los derechos que poseen los usuarios y las obligaciones y deberes que deben respetar quienes manejan estos datos de ubicación a los cuales nos referiremos en este estudio.

PALABRAS CLAVE: geolocalización, derechos de la personalidad, privacidad, protección de datos.

ÍNDICE

I.- INTRODUCCIÓN

El presente trabajo tiene por objeto el análisis jurídico de algunas de las implicaciones de la obtención de la ubicación de las personas, ya que existe una relación directa con la esfera privada personal y la protección de datos. Este estudio, desde nuestro punto de vista, es clave para atender a una de tantas necesidades sociales que surgirán en un futuro, pues nuestra privacidad es una de las cuestiones que más se ha puesto en entredicho a raíz de nuestra evolución social y tecnológica. Frente a la actual era digital que busca y promueve que tengamos un perfil digital, nuestro ordenamiento jurídico debe reaccionar para garantizar la protección constitucional de los derechos fundamentales y otros bienes jurídicos protegidos.

Actualmente, existe una gran diversidad de avances tecnológicos que en mayor o menor medida han incidido en nuestra vida y, por ende, en nuestra privacidad. Entre estos se encuentran las técnicas de geolocalización con las que cuentan la mayoría de dispositivos móviles. Dada su gran cantidad de aplicaciones no es de extrañar el hecho de que se utilice también para su uso en las redes sociales[1] y no sólo en lo que a la navegación y búsqueda de lugares se refiere. La cuestión es que se hace al usuario más participativo en cualquier plataforma; idea que tiene su precedente en la Web 2.0[2] o web social; evolución de la Web 1.0 que era principalmente estática. Todo comienza a partir del año 2003 cuando se empiezan a desarrollar la mayoría de redes sociales más importantes en este momento, como MySpace y Linkedin en ese año y Flickr y Facebook en 2004. Es entonces cuando los internautas, siendo antes solo consumidores de contenido, ahora empiezan a crearlo, a compartir y a comentar; en definitiva, a ser más activos y participativos. Ya no solo afecta a los nativos digitales sino que nos hemos convertido en una generación 2.0 que cada vez, en menor medida, puede hacer frente a su día a día sin mantenerse conectado.

[1] El Dictamen 5/2009 sobre las redes sociales en línea adoptado por el Grupo de Trabajo sobre protección de datos del artículo 29 define las redes sociales o servicio de red social (SRS) como "*plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información…*".

[2] La Web 2.0 es un concepto utilizado por Tim O'Reilly por primera vez en 2004 en una conferencia y posteriormente en su blog en 2005. Este es el artículo donde explica la Web 2.0. http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html última consulta: 21.06.2017.

La parte negativa de la geolocalización radica en el hecho de que haya despertado una serie de usos indebidos dado el atractivo que supone para las compañías el conocer las preferencias y los sitios frecuentados por sus usuarios (lo que se ha empezado a denominar *trazabilidad vital* o *patrón de conducta*). Esta información que viene a ser de gran interés para las empresas ha hecho que podamos constatar que son generalmente las aplicaciones gratuitas las que suelen solicitar acceso a la ubicación[3] porque básicamente obtienen sus beneficios a través de la venta de esta información. Podemos determinar que en estos casos, en vez de usuarios, somos el producto de empresas que se benefician a nuestra costa.

Al hilo de esto, cuando comenzamos a utilizar una aplicación de este estilo estamos consintiendo el acceso a nuestra ubicación, pero incluso cuando no prestamos esta voluntad también nos podemos ver perjudicados. Como ejemplo de esto último, el año pasado una compañía telefónica envió a sus clientes un SMS en mayo de 2016 con el motivo de informar de que iban a proceder a tratar los datos de tráfico de internet y ubicación de las comunicaciones de sus dispositivos móviles. Pero, además, se indicaba a los usuarios que si en el plazo de 30 días no manifestaban su oposición, la empresa entendía que se había otorgado el consentimiento para el tratamiento de datos. Ante esto, la Agencia Española de Protección de Datos (AEPD) ha permitido que esta empresa de telefonía recabe datos de geolocalización de los terminales de sus clientes sin que sea precisa la obtención de su consentimiento, requisito que como veremos más adelante es necesario[4]. Interesa subrayar, por tanto, que la geolocalización en sí no es un problema, pues es solo otra técnica más, producto del desarrollo tecnológico; lo significativo es su relación con nuestra privacidad.

A continuación analizaremos lo que se entiende por geolocalización y además profundizaremos en lo que viene siendo nuestro objetivo, que es el de tratar la injerencia que supone en los derechos de la personalidad, así como lo relativo a la protección de

[3] http://tecnologia.elpais.com/tecnologia/2017/03/27/actualidad/1490626770_125439.html última consulta: 21.06.2017.
[4] http://huelvared.com/2017/01/15/la-aepd-permite-a-movistar-recoger-la-geolocalizacion-de-los-moviles-en-contra-del-criterio-europeo/ última consulta: 21.06.2017.

datos, ya que nos estamos refiriendo a datos de índole personal, por lo que debemos examinar cuestiones como el consentimiento ante esta relación jurídica, los sujetos implicados, las obligaciones y deberes del responsable y los derechos del usuario. Conjuntamente trataremos de ofrecer posibles vías de protección desde el punto de vista del usuario, que, en último término, podría ser el perjudicado en estas relaciones.

II.- CONCEPTO Y DELIMITACIÓN DE LA GEOLOCALIZACIÓN

La geolocalización puede definirse como *"la tecnología que permite ubicar un dispositivo en un punto espacial a partir de la transmisión de sus coordenadas de posicionamiento"*[5], pero en realidad es más que eso, pues técnicamente *"hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (x), longitud (y) y altura (z)"*[6]. Actualmente la Real Academia Española (RAE) no ofrece un concepto de geolocalización, el término más similar es *localizar*[7], por el que podemos afirmar que el objetivo más básico de la georreferenciación es el de localizar a una persona, aunque no el único. Respecto a la forma por la que se obtiene la ubicación, se utiliza lo que se conoce como GPS, sigla de Global Positioning System o Sistema de Posicionamiento Global, que la RAE define como *"sistema que permite conocer la posición de un objeto o de una persona gracias a la recepción de señales emitidas por una red de satélites"*. Entre los dispositivos que integran esta tecnología tenemos los *smartphones*[8], *smartwatches*[9] y tabletas[10] en los

[5] BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015, p. 48.
[6] BELTRÁN LÓPEZ, G. «La geolocalización social». *Polígonos, Revista de geografía*, nº27, 2015, p. 104.
[7] Definición de *localizar* por la RAE:
1. tr. Fijar, encerrar en límites determinados.
2. tr. Averiguar el lugar en que se halla alguien o algo.
3. tr. Determinar o señalar el emplazamiento que debe tener alguien o algo.
[8] Smartphone no ofrece definición en la RAE pero lo entendemos como "*teléfonos móviles inteligentes de última generación que aprovechan la miniaturización de todos los componentes y ofrecen una más rápida y efectiva conexión, distinguiéndose por la cantidad de utilidades que tienen para los usuarios, incluyendo correos electrónicos capaces de cualquier transmisión de datos. Estos teléfonos celulares son casi mini computadoras portátiles, al punto de contar con un sistema operativo que permite la instalación de aplicaciones propias de internet*".
http://www.movieonmovil.com/glosario-de-celulares.html#S última consulta: 21.06.2017.

que se va un paso más allá de la información que puede ofrecer un ordenador, un *router*[11] o incluso un automóvil con GPS. La forma de obtener la ubicación se basa en la obtención de la posición a través de la triangulación de las señales de satélites que orbitan la Tierra[12] y de los repetidores de las antenas de telefonía que también permiten obtener la ubicación de sus clientes a través de las conexiones de los dispositivos a sus estaciones base. Por así decirlo, existen dos vías para determinar la localización de un dispositivo: a través de las señales de los satélites y por medio de las estaciones base o antenas de telefonía a las que nuestros dispositivos se conectan a través de Wifi o por datos móviles (3G o 4G). Será, en este último caso, más sencilla la localización si se encuentra en un lugar donde confluyan mayor número de antenas de telefonía[13].

Una vez determinada cómo funciona la georreferenciación, conviene advertir una serie de usos de la misma que nos ayudará a entender la importancia de esta técnica y la posible intromisión en la privacidad antes de continuar con el análisis jurídico. Nos centraremos en aplicaciones para teléfonos inteligentes, ya que es donde más se aplica la georreferenciación y de dónde más información se puede extraer de los titulares[14]. Basándonos en un estudio personal acerca de los diversos empleos de la geolocalización podemos clasificar sus funciones de la siguiente manera:

1º. Fines de seguridad: cuando se utiliza la ubicación con fines de socorro como para encontrar a una persona que se ha perdido o ha sufrido un accidente. Existen

---

[9] Un Smartwatch es "*un dispositivo que toma la forma de un reloj de pulsera, pero que internamente cuenta con un hardware de un dispositivo móvil como un Smartphone, lo que le permite correr aplicaciones y conectarse con el mundo exterior*". http://www.definicionabc.com/tecnologia/smartwatch.php última consulta: 21.06.2017.

[10] Tablet tampoco aparece en la RAE y es un ordenador portátil "*más grande que un Smartphone pero, generalmente, más pequeña que una netbook. Se caracteriza por contar con pantalla táctil*". http://definicion.de/tablet/ última consulta: 21.06.2017.

[11] Un Router "*se encarga de establecer qué ruta se destinará a cada paquete de datos dentro de una red informática. Puede ser beneficioso en la interconexión de computadoras, en la conexión de los equipos a Internet o para el desarrollo interno de quienes proveen servicios de Internet*". http://definicion.de/router/ última consulta: 21.06.2017.

[12] http://www.abc.es/tecnologia/moviles-telefonia/20140320/abci-localizacion-movil-201403192024.html última consulta: 21.06.2017.

[13] http://www.elconfidencial.com/tecnologia/2016-10-22/telefono-movil-localizacion-datos-wifi-antenas_1278503/ última consulta: 21.06.2017.

[14] En contraposición, un ordenador, por ejemplo, no está constantemente encendido ni está continuamente con nosotros en la mayoría de los casos por lo que no podría obtenerse la denominada trazabilidad vital de una persona.

aplicaciones[15] que obtienen datos de los centros de atención de llamadas o servicios de emergencias del país en que nos encontramos y permite enviar la ubicación a los mismos.

2º. Mapeo y rutas: una de las más populares y utilizadas es Google Maps aunque también encontramos TomTom y otras específicas que imitan guías de viajes para turistas (ej. Tourist Eye) o también para senderistas como Naturapps. Pero sin duda para recorrer ciudades la aplicación más innovadora entre los usuarios es FourSquare. Esta última es la más destacada en cuanto a la gran cantidad de información que gestiona, tanto personal, como de ubicación, gustos y preferencias. Básicamente es una red social que sirve para "contar" en todo momento dónde estamos, que sitios nos gustan y dar una valoración de los mismos. Cuanto más *check-in*, comentarios y/o valoraciones de visitas a lugares hayamos hecho, más popularidad vas obteniendo hasta convertirte en "alcalde" por lo que te conviertes en un referente para otros usuarios. Además, puedes ver en tiempo real contactos que están cerca de ti para poder comunicarte con ellos (mediante la aplicación asociada Swarm).

3º. La geolocalización en redes sociales y el geoetiquetado: cuando son las propias redes sociales las que animan a que compartamos fotografías, imágenes, vídeos o publicaciones acompañando nuestra ubicación o la ubicación de donde se tomó este contenido en dicho momento. Por lo que respecta al geoetiquetado[16] o etiquetado geográfico específico sirve para agregar información de ubicación en los metadatos[17] de archivos de imágenes, vídeos, sonido, sitios web, entre otras formas. Así conoceríamos desde donde fue tomada y dado que una gran cantidad de redes sociales promueven su uso y muchos usuarios suben estos contenidos en el mismo momento en el que fueron tomados se puede conocer la ubicación de una persona al instante. Aparte del volumen de información que puede obtenerse entrelazando la información del perfil junto con la

[15] Como ejemplo de ello tenemos *Help me SOS international*.
[16] Geoetiquetado o geotagging http://geografia.laguia2000.com/general/geoetiquetado última consulta: 21.06.2017.
[17] Los metadatos se pueden definir como "el conjunto de datos de los productos geográficos (datos y servicios web) que permite a su productor de describir todas las características (título, formato, fechas,…) y a los usuarios utilizar adecuadamente esos productos" http://metadatos.ign.es/# última consulta: 21.06.2017.

ubicación, también llama la atención que podamos buscar un determinado lugar y ver todo el contenido que se ha publicado y este asociado a ese espacio.

4º. Geomarketing: cuando se saca provecho de la geolocalización para ofrecer productos, servicios, promociones o crear publicidad de forma mucho más acorde con los gustos y preferencias de los usuarios. Se trata de una utilidad específica de la geolocalización entendida como técnica publicitaria[18] por la que se pueden aumentar y mejorar las estrategias y acciones que tengan que ver con la comunicación y el marketing[19]. En esta categoría también conecta Foursquare y afecta a los establecimientos comerciales que perderán clientes si no están al tanto de la misma porque los usuarios no podrán valorarlos y así posicionar favorablemente los mismos. Dejando a un lado esta multifacética aplicación, en el resto de redes es bastante frecuente encontrar publicidad atendiendo a las búsquedas, lo cual también es intrusivo y muchas veces sorprende ver ofertas tan específicas a tus preferencias.

5º. Jugabilidad: un gran número de aplicaciones para juegos la utilizan, una de las más conocidas es Pokemon Go[20]. Respecto a este juego se hace eco BIURRUN ABAD acerca de las "*imprudencias de los jugadores y las infracciones legales*" [21] que han acontecido desde que se lanzó al mercado y no es para menos, ya que se ha promovido la creación de aplicaciones no oficiales que resultaron ser maliciosas aprovechándose de "*la fama del juego y así poder obtener datos personales*". Ante esto, sus creadores ya se han percatado de los posibles peligros que conlleva y ahora ofrecen más advertencias sobre no conducir vehículos y utilizar la aplicación, no entrar en propiedades privadas, entre otras advertencias. Algún autor ha señalado que "*la aplicación recoge la*

[18] Como ejemplo de uso del geomarketing tenemos la aplicación de McDonald's que te avisa para que actives tu GPS para así ofrecerte ofertas personalizadas a tu zona.
[19] LÓPEZ JIMÉNEZ, D. DITTMAR, E. C. "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital" en VALERO TORRIJOS, J. *La protección de los datos personales en internet ante la innovación tecnológica*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 527.
[20] En estos juegos se combina la realidad aumentada y la georreferenciación que "*se basa en la superposición de información virtual sobre un determinado objeto o imagen de forma digital*". Así la podemos distinguir de la realidad virtual "*que no sustituye la realidad física, sino que sobreimprime los datos informáticos al mundo real*"[20] consiguiendo el usuario una mejor experiencia.
[21] BIURRUN ABAD, F.J. «Pokemon Go y su impacto en la "legalidad aumentada"», *Actualidad Jurídica núm. 922*, Ed. Aranzadi, Cizur Menor, 2016, pp. 1-3.

geolocalización exacta y detallada del usuario, y mientras juega y camina por la ciudad, envía información sobre su ubicación, lo que permite a sus creadores poseer un mapa exacto sobre sus hábitos y movimientos […] a dicha información se sumaba la posibilidad de acceso por los desarrolladores a toda cuenta Google de los usuarios"[22].

6º. Aplicaciones para establecer contactos: como ejemplo tenemos Tinder, Badoo o Lovoo que como resulta evidente son de las que más interfieren en los derechos a la propia imagen, intimidad y protección de datos, ya que los usuarios deben obligatoriamente poner una foto de perfil e indicar su nombre, edad, intereses, entre otros datos para poder hacer un uso completo de la aplicación y validar su perfil. Este sistema de reconocimiento también exige que activen su ubicación para poder ver a los contactos que tienen cerca y que también son usuarios de dicha aplicación.

7º. Localizar mascotas y objetos: a través de pequeños dispositivos rastreadores que se conectan con nuestro teléfono u ordenador y nos señala en el mapa donde está ubicado. Estos dispositivos pueden esconderse perfectamente en la ropa o pertenencias de alguna persona para también tenerla localizada, lo cual sería bastante intrusivo.

Cuando dejamos a un lado las aplicaciones oficiales, que se obtienen en plataformas de distribución digital como Play Store o App Store, podemos encontrarnos con otras no tan conocidas pero que son de las más intrusivas. Como ejemplo de ello tenemos "NSA Photo Spy", esta aplicación permite el acceso a fotos publicadas por usuarios cerca de tu ubicación, incluso desde otras aplicaciones como Flickr, Instagram, Pinterest, etc., pero se trata de una aplicación no oficial por lo que debemos evitar su uso y tampoco será objeto de atención.

Por todo lo expuesto y teniendo presente las formas por las que obtenemos de los usuarios los datos de ubicación abordaremos a continuación el estudio de la afección en la intimidad personal y protección de datos. La relación que existe entre estos dos

[22] BIURRUN ABAD, F.J. «Pokemon Go y su impacto en la "legalidad aumentada"». *Actualidad Jurídica núm. 922*, Ed. Aranzadi, Cizur Menor, 2016, pp.1-3.

últimos aspectos es consecuencia directa de la utilización de aplicaciones o tecnología que permite el posicionamiento de forma inmediata de los individuos, intentando, en la medida de lo posible, considerar los aspectos problemáticos y ofrecer posibles indicaciones o soluciones, al igual que determinar si la regulación es suficiente y además precisa en este aspecto en concreto.

III.- DERECHOS DE LA PERSONALIDAD Y LA PROTECCIÓN DE DATOS EN RELACIÓN A LA GEOLOCALIZACIÓN

1.- Derechos de la personalidad que pueden verse vulnerados y la incidencia de las TIC en los mismos

Analizaremos en concreto los que pueden verse vulnerados a raíz de la utilización de los datos de geolocalización como son el derecho al honor, la intimidad personal y familiar. Nos estamos refiriendo a los derechos de la personalidad más la suma de otros derechos instrumentales a estos, como el derecho a la autodeterminación informativa y el derecho al olvido. Estos últimos son los que más han evolucionado como consecuencia de las TIC, es decir, la Tecnología de la Información y Comunicaciones que ha tenido un gran impacto es nuestra sociedad, cultura y hábitos[23] al igual que en la privacidad.

Los derechos que pueden verse lesionados son aquellos que se vinculan a la esfera más personal de los seres humanos por lo que se consideran derechos subjetivos peculiares -por su objeto, caracteres y contenido-. En los mismos concurren varias características que es importante destacar: son inherentes al ser humano, cuestión que deriva del principio que inspira a todo el ordenamiento jurídico, es decir, la dignidad de la persona reconocida en el artículo 10 de la Constitución española (en adelante, CE). Por ello, se trata de derechos innatos u originarios, no transmisibles e imprescriptibles. A su vez, son derechos absolutos oponibles frente a todos; extrapatrimoniales ya que son personales, al igual que indisponibles e irrenunciables[24].

[24] DE PABLO CONTRERAS, P., *Curso de Derecho Civil I. Volumen II. Derecho de la Persona*, reimpresión de la 5ª edición., Ed. Edisofer, 2016, pp. 263-278.

En primer lugar, analizaremos el derecho a la intimidad por su especial relación con el tema que tratamos, seguido del derecho a la autodeterminación informativa que consideramos que deben ir de la mano para garantizar una protección completa a los usuarios.

1.1.- El derecho a la intimidad

Este derecho se configura en el artículo 18.1 CE por el que "*se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*". Aunque en el precepto constitucional se contenga el derecho al honor y a la propia imagen nos centraremos en el derecho a la intimidad por su especial relación con este tema[25], como ya hemos indicado.

Debemos recalcar que el derecho a la intimidad personal y familiar y a la propia imagen, según la Sentencia del Tribunal Constitucional de 28 de enero de 2003 (fundamento jurídico cuarto)[26], son tres derechos autónomos y sustantivos, aunque se encuentran estrechamente vinculados entre sí, al tratarse de derechos que derivan de la dignidad humana y están enfocados a proteger el patrimonio moral de las personas. Por su parte, el derecho al honor protege la favorable reputación de un individuo ante cualquier tipo de expresiones que pudieran menoscabar la valoración o consideración ajena. No solo se desenvuelve hacia lo que opinen los demás de alguien sino también de forma introspectiva (o estimación propia), es decir, cuando la propia estima se ve afectada sin que sea necesario que la intromisión afecte a la consideración ajena de dicha persona. Asimismo, el derecho a la propia imagen entendido como la facultad de disposición de la información gráfica acerca de su persona a la hora de ser captada o que

[25] GARRIGA DOMÍNGUEZ, A. (coord.), *Fundamentos Éticos y Jurídicos de las TIC*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2012, p. 67-68.

[26] RJ 2003/14. En el fundamento jurídico cuarto se dispone que el "*carácter autónomo de los derechos del art. 18.1 CE supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros dos derechos fundamentales que prevé este precepto constitucional, pues la especificidad de cada uno de estos derechos impide considerar subsumido en alguno de ellos las vulneraciones de los otros derechos que puedan ocasionarse a través de una imagen que muestre, además de los rasgos físicos que permiten la identificación de la persona, aspectos de su vida privada, partes íntimas de su cuerpo o que se la represente en una situación que pueda hacer desmerecer su buen nombre o su propia estima*".

pueda tener difusión pública difícilmente desde nuestro tema podrá verse afectado, por ello, no será necesario su análisis.

La intimidad va a ser el derecho que examinaremos más en profundidad pues es el que, en mayor medida, se vincula a la preservación del ámbito privado de las personas que desea mantenerse oculto de cara a los demás, ya que los datos personales de ubicación pueden afectar a este derecho como ya veníamos adelantando. El mencionado derecho se une a la dignidad y el libre desarrollo de la personalidad (art. 10.1 CE) como el resto de derechos de la personalidad, pero juega un papel más determinante que el resto de derechos. No solo reconoce a la persona individualmente considerada, pues se configura como el poder de resguardar su ámbito más privado y no solo personal, sino también al núcleo familiar. Es importante entender que la intimidad no va a suponer solamente que se aleje del conocimiento ajeno de la esfera que rodea a esa persona, sino que también comprende la *"necesidad de un ámbito de desenvolvimiento interior como instrumento imprescindible para el pleno desarrollo de la libertad individual*"[27]. Igualmente incluye cualquier tipo de información relativa a un individuo que pueda afectar a su intimidad siempre y cuando su titular pretenda alejarla de la curiosidad ajena. Esto no implica que sea un derecho ilimitado, pues no puede ser considerado individualmente sino que debe ponderarse junto con otros valores de la sociedad a la hora de determinar si una concreta información debe ceder ante otros intereses. Existen valores que predominan, como es el interés público, pero, en definitiva la intimidad no es solo información, sino un espacio ("intimidad territorial"[28]), de ahí que se encuentre en relación con la inviolabilidad del domicilio[29] y el secreto de las comunicaciones[30].

[27] HERRÁN ORTIZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales*, Ed. Dykinson, Madrid, 2002, p. 19.
[28] MIERES, L.J., *Intimidad Personal y Familiar* (prontuario de Jurisprudencia Constitucional), Ed. Aranzadi, 2002, p. 49.
[29] En cuanto a la inviolabilidad del domicilio también puede, de forma indirecta, verse comprometida con el uso de la ubicación cuando compartimos nuestra ubicación o etiquetamos un contenido a un determinado lugar dejando entrever que no nos encontramos en nuestro domicilio. Si bien es un tanto forzada esta afirmación la cuestión es que podría existir un nexo entre un allanamiento de morada y la información que compartimos públicamente en la red.
[30] GRIMALT SERVERA, P. *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, 1ª edición, Ed. Iustel, 2007, pp. 34-35.

A su vez, la intimidad tiene relación con la privacidad; pues bien, estos dos conceptos han sido objeto de debate y conviene advertir su distinción. La privacidad era considerada como la libertad que tiene el individuo frente al contacto con la sociedad y la observación de terceros, separándose, por tanto, de la intimidad. Este debate ya está superado y se entiende que la privacidad es un concepto más amplio que viene a proteger un bien jurídico diferenciado de la intimidad en lo que se refiere a aspectos de un individuo considerados en su conjunto, pues si se tienen en cuenta de forma aislada no serían tan relevantes. Si la privacidad es entendida como el derecho a "*mantener inaccesible al conocimiento, curiosidad y crítica de terceras personas*", la intimidad, como ya veníamos diciendo, defenderá solo la esfera más reservada de los individuos. Ambos conceptos ofrecen aspectos complementarios, por lo que para poder alcanzar una protección completa de un individuo ante las posibles amenazas de las TICs solo se alcanzará a través de la tutela conjunta de estas esferas de actuación[31].

El amparo que ofrece lo configura como un derecho que se hace valer frente a la actuación y conocimiento de los demás tanto si son particulares como poderes públicos[32]. Este derecho tiene dos contenidos, uno positivo y otro negativo[33], el primero referido al control de la información personal para evitar intrusiones en nuestra intimidad sin nuestro consentimiento y el negativo en lo referido a la exclusión de terceros y la prohibición de la divulgación[34]. En el propio contenido de la intimidad también se encontraría la privacidad como facultad que integra el propio derecho a la intimidad y que si cabe puede considerarse a la privacidad como una defensa preventiva de los riesgos que proceden del uso de la informática para que no lleguen a vulnerar el derecho primordial.

[31] HERRÁN ORTIZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales*, ed. Dykinson, Madrid, 2002, pp. 44-45.
[32] En palabras del Tribunal Constitucional "*la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana*" (en el fundamento jurídico tercero de la Sentencia del Tribunal Constitucional del 2 de diciembre de 1988 RJ 1988/231).
[33] Hay autores que establecen dos contenidos, uno denominado libertad negativa y otro libertad positiva, como HERRÁN ORTIZ.
[34] GRIMALT SERVERA, P. *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, 1ª edición, Ed. Iustel, 2007, p. 30 y ss.

Principalmente, es consecuencia del uso informático que el derecho a la intimidad, considerado como un derecho flexible, haya evolucionado. Debe posibilitarse la adaptación a los constantes cambios como consecuencia de la evolución social, tecnológica y cultural, cambios que hoy en día ha motivado a que integre un contenido más amplio que el que en un primer momento se había previsto (sentencia del Tribunal Constitucional del 12 de noviembre de 1990)[35]. Es fundamento, además, por el que no debería ofrecerse un concepto cerrado del mismo, porque podría dejarse fuera contenido que debería incluirse y porque está en constante progreso y transformación[36]. Asimismo, las intromisiones que pueden efectuarse como consecuencia de las formas de captación, divulgación y difusión son mucho más sencillas y al alcance de todos que las que había hace décadas.

Desde nuestro punto de vista, la intimidad está mucho más comprometida hoy en día y por ello debe afianzarse aún más la protección, dado que una gran cantidad de acciones pueden considerarse como intromisiones legítimas e ilegítimas. Como bien indica el Dictamen del grupo de trabajo del articulo 29 acerca de los riesgos para la intimidad, estos datos permiten a proveedores –de los servicios de georreferenciación- obtener "*una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos"* así como integrar los datos de sus contactos para obtener una "*gráfica social*", al igual que se puede agregar "*categorías especiales de datos, por ejemplo visitas a hospitales y lugares de culto, presencia en actos políticos o en otros lugares específicos que, verbigracia, revelen datos sobre la vida sexual. Estos perfiles pueden ser utilizados para tomar decisiones que afecten significativamente a su propietario*". Sobre esta monitorización constante indica el Grupo de Trabajo que este seguimiento se puede hacer de forma secreta "*sin informar al propietario*" o semisecreta cuando el usuario "*olvida*" o no está informado de que

[35] RJ 1990/171. Esta sentencia en el fundamento jurídico cuarto determina que el derecho a la intimidad y al honor "*son realidades intangibles cuya extensión viene determinada en cada sociedad y en cada momento histórico y cuyo núcleo esencial en sociedades pluralistas ideológicamente heterogéneas deben determinar los órganos del Poder Judicial. Esta delimitación de los hechos y de sus efectos es el punto de partida para el juicio de este Tribunal*".
[36]GARRIGA DOMÍNGUEZ, A. (coord.), «Fundamentos Éticos y Jurídicos de las TIC» en "*El impacto de las TIC en los derechos humanos*", 1ª edición, Ed. Aranzadi, Cizur Menor, 2012, p. 73.

estén activados los servicios de localización o los parámetros de accesibilidad se hayan cambiado de privado a público[37].

1.2.- Derecho a la autodeterminación informativa

Partiendo del derecho a la intimidad que se reconoce en el artículo 18.1 CE derivan otra serie de derechos que son instrumentales a este y son: la inviolabilidad del domicilio del artículo 18, el secreto de las comunicaciones del apartado tercero del mismo artículo y la autodeterminación informativa del art. 18.4. Sobre este último derecho, dicho artículo establece que "*la ley limitará 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*". Como podemos apreciar, el precepto no lo denomina autodeterminación informativa, sólo se ciñe a señalar ésta limitación al uso de la informática como si fuese algo accesorio únicamente.

Por su parte, el propio Tribunal Constitucional lo denomina *libertad informática* por lo que estos conceptos son sinónimos. La sentencia que data del 20 de julio de 1993 (fundamento jurídico sexto[38]) fue la primera en la que el Tribunal Constitucional se pronuncia sobre este derecho y afirma que es autónomo del derecho a la intimidad, y posteriormente en la Sentencia de 30 de noviembre del 2000, ya que el derecho a la intimidad personal y familiar protege cualquier invasión en dicho ámbito que esa persona quiera excluir del conocimiento ajeno mientras que el derecho a la protección de datos "*persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*", de ahí que su objeto sea diferente dando respuesta a "*una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona*" (fundamento jurídico sexto[39]) como es la libertad informática. Asimismo, incluye cualquier tipo de datos personales incluso públicos que identifiquen o puedan

[37] Se hace referencia en la página 7 del Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes.
[38] RJ 1993/254.
[39] RJ 2000/292.

identificar al ciudadano. Este derecho es instrumental, por tanto, sirve de garantía de otros derechos ya sean o no constitucionales.

En su contenido se puede distinguir un elemento negativo y positivo, el primero es referido a la literalidad del artículo 18.4 acerca de "*limitar el uso de la informática*" para garantizar el honor, la intimidad y el pleno ejercicio de los derechos de los ciudadanos[40]. Es decir, el contenido negativo se refiere a las cautelas y, como propiamente indica, límites al procesamiento de datos. Mientras que el positivo se refiere al control sobre los datos relativos a la propia persona, es decir, el *habeas data*[41]. El *habeas data* o también llamado como *habeas scriptum* consiste "*en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos*" (fundamento jurídico quinto[42]). Este término que tiene su paralelismo con el *habeas corpus* que si este supone el control de la libertad personal, el habeas data va a suponer el control de los datos informáticos.

Dado que los datos personales son un bien jurídico protegido y además susceptible de tráfico jurídico, y precisamente para salvaguardar los intereses de los usuarios, entiende BATUECAS CALETRÍO que aquellos 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*"[43]. Es decir, el recorrido que habitualmente sigue en su vida diaria -y que puede indicarnos su domicilio, su lugar de trabajo o incluso lugares de entretenimiento que frecuenta-. Esta información excede en grandes proporciones el destino que el usuario desea de estos

[40] Como establece la propia sentencia "*la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos 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*".
[41] GARRIGA DOMÍNGUEZ, A. (coord.), «Fundamentos Éticos y Jurídicos de las TIC», 1ª edición, Ed. Aranzadi, Cizur Menor, 2012, p. 78-79.
[42] RJ 2000/292.
[43] BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015, p. 60.

servicios y supone, por tanto, una intromisión en su intimidad. En definitiva este derecho sirve de garantía a los individuos para poder controlar sus datos, básicamente para no ser tan accesibles ante terceros.

La evolución de este derecho no solo está contenida en la Ley de Protección de Datos pues ha pasado por varias etapas de regulación. En la primera etapa ya se empezó a exigir la autorización previa para la creación y funcionamiento de ficheros de datos personales al igual que límites en la utilización de la informática. En la segunda etapa, en este aspecto, se define por la permisividad en los tratamientos de datos, sólo protegiendo en mayor medida los datos que fuesen más sensibles o de un interés especial. En cuanto a la tercera etapa se empieza aquí con una línea que busca el equilibrio entre el derecho a la información y la protección de datos personales. En esta última etapa se encuadra la Directiva 95/46/CE que ya hemos nombrado y que fue el motivo por el que se reformó gran parte del derecho interno de los países europeos; en el caso de España se aprobó la LOPD en 1999[44]. La cuarta etapa debe estar definida por una mayor autonomía de los afectados por el tratamiento de datos y centrándose en la principal fuente de obtención de estos datos que es a través de internet. Como consecuencia directa de la posible obtención de datos especialmente sensibles que necesitan una correlativa especial atención. Nos referimos a los del artículo 7 de la LOPD que pueden revelar información acerca de la ideología, afiliación sindical, religión y creencias.

1.3.- Derecho al olvido

Este derecho ha sido objeto de debate en estos últimos años a raíz de que no existe un concepto sobre el mismo. En palabras de COBAS COBIELLA este derecho es definido como "*derecho al deshonor*" y es entendido como la facultad que tenemos para que "*nuestro pasado sea enterrado, que no sea reabierto y que hechos que sucedieron*

[44] HERNÁNDEZ LÓPEZ, J.M., «El Derecho a la Protección de Datos Personales en la doctrina del Tribunal Constitucional» en "*Origen y fundamento del derecho a la protección de datos personales"*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2013, pp. 25-26.

en el pasado, y que habían sido olvidados, no se vuelvan a divulgar"[45]. Este concepto aunque este más encaminado a la protección *post mortem* del derecho al honor a través del derecho al olvido nos ayuda a entenderlo.

Tiene su origen en algunas resoluciones dictadas en Estados Unidos en las que se trató de limitar la libertad de prensa invocando el derecho al olvido, pero la respuesta de los tribunales se inclinaba porque prevaleciera la libertad de información siempre y cuando existiera un interés público y dicha información fuera veraz. Línea que ha seguido el Tribunal Constitucional por la prevalencia de garantizar la libertad de información y expresión para que sirva en la formación de una opinión pública libre. También entiende el Tribunal Constitucional que la libertad de expresión e información no pertenecen únicamente a los medios de comunicación sino a cualquier ciudadano, de ahí que internet venga a consolidar el derecho reconocido en el artículo 20 CE. De esta manera se puede afirmar que estas libertades solo se condicionan por la veracidad de la información y que supone un límite para el derecho al honor, la intimidad o la propia imagen, por ello, prevalecerá si tiene un interés público[46].

El derecho al olvido viene a ser justo lo contrario a lo expuesto, va a limitar la libertad de expresión a favor de la protección del individuo respecto de aquella información que aparezca en la red; específicamente cuando se hiciesen referencias sobre algunos aspectos de su vida en internet que independientemente del origen o veracidad pudiesen repercutir negativamente en su desarrollo personal[47].

La regulación del derecho al olvido viene establecida en el artículo 17 del Reglamento Europeo[48] que lo denomina, a su vez, derecho de supresión por el que se

[45] COBAS COBIELLA, M.E. Derecho al olvido. Comentando algunas cuestiones. En *Derecho al Honor: Tutela Constitucional, Responsabilidad Civil y Otras Cuestiones*, DE VERDA Y BEAMONTE, J.R. (coord.), 1ª edición, Ed. Aranzadi, Cizur Menor, 2015, p. 231.
[46] APARICIO SALOM, J., Elemento formal. Constitución del tratamiento. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, pp. 310-311.
[47] APARICIO SALOM, J., Elemento formal…, ob. cit. p. 311.
[48] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

obliga al responsable a suprimir los datos personales a solicitud del interesado cuando: estos datos personales no sean necesarios para los fines iniciales; el interesado retire el consentimiento; se oponga al tratamiento; los datos personales hayan sido tratados ilícitamente; estos datos deban suprimirse como consecuencia de una obligación legal; y cuando estos datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información en relación a las condiciones para la prestación del consentimiento en menores.

Vendría a ser el derecho al olvido una manifestación específica de la obligación de destrucción de datos y cómo resume APARICIO SALOM[49] en los casos en que ya no son necesarios porque no sirven para la finalidad destinada, porque el interesado ha procedido a revocar su consentimiento, porque ha ejercido el derecho de oposición o porque este tratamiento infringe el propio Reglamento Europeo.

Sobre el conflicto entre el derecho a la información y el derecho al olvido, en el apartado segundo del artículo 16 de la LOPD se establece que el responsable del tratamiento puede oponerse a la cancelación si existe alguna razón de interés que prevalece frente al derecho al olvido en favor de la libertad de expresión. A su vez, exige que el responsable principal comunique a responsables ulteriores del tratamiento de esos datos personales –es decir, a los que se ha cedido información- para que también supriman dichos datos (copias, enlaces, etc.)-. En este caso sí se estaría restringiendo la libertad de expresión porque no existe ninguna vía de oposición ni de intervención judicial[50]

La complejidad para los perjudicados a la hora de ejercer el derecho al olvido cuando la información publicada puede ampararse en el derecho a la libertad de expresión e información, ha motivado a que la AEPD en vez dirigirse al autor del contenido se dirija a los buscadores de internet para que oculten esta información[51]. Uno

[49] APARICIO SALOM, J., Elemento formal…, ob. cit. p. 311.
[50] APARICIO SALOM, J., Elemento formal…, ob. cit. p. 312.
[51] Entre las criticas como bien señala APARICIO SALOM se basan en que la AEPD "intenta atajar las dificultades amparando a los ciudadanos que solicitan la protección de sus datos, lo que resultaría loable

de los casos más importantes fue el de Google Spain contra la AEPD que se resuelve en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014[52] en el que el afectado había aparecido en una noticia en relación a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social, sobre lo que el TJUE consideró que estos datos tenían carácter sensible porque se identificaba por su nombre al afectado y que dicha publicación era antigua (se remontaba 16 años atrás) y por todo ello tiene derecho[53] a que no se siga vinculando con su persona porque no existe un interés público para que prevalezca esta información[54]. Como no se dirigía frente al redactor de la noticia sino al buscador Google, se justificaba en que la "*actividad de un motor de búsqueda, que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del mencionado artículo 2, letra d)*" (apartado 100.1).

Nos hace reflexionar esta cuestión sobre la verdadera responsabilidad del sujeto que se dedica a indexar información únicamente que otros usuarios crean, pues si se tratase de un blog personal es más comprensible el control de los comentarios, pero aquí estamos haciendo responsable a una compañía que solo hace más accesible la información. No es realmente efectivo el "ocultar" la información porque el contenido seguirá estando ahí pero no de los primeros resultados, de igual forma, si indagamos un poco más podremos acceder. Esta sentencia ha sido criticada y entre ellas tenemos la crítica de Enrique DANS que considera que esta resolución "*no elimina realmente la*

si su actuación no vulnerara las garantías constitucionales de las libertades de información y expresión, no invadiera la competencia reservada a los tribunales, no impidiera al autor defender sus derecho al no actuar frente a él y no derivara indebidamente la responsabilidad al actuar frente a los buscadores. Para mayor crítica, la Agencia infringe además los límites territoriales de competencia" p. 313.

[52] RJ 2014/85.

[53] En este caso se hacía valer el cumplimiento del artículo 12. b) (derecho de rectificación, supresión o bloqueo) y 14.a) (derecho de oposición)

[54] Apartado 98 de la sentencia acerca de la tercera cuestión prejudicial.

información ciudadana del buscador, sino que anima a conseguirla por otros medios […] nadie puede obligar a nadie a olvidar ya que regular es censurar"[55].

Cuesta encontrar resoluciones que estimen el derecho al olvido y es que la línea del Tribunal Constitucional es la de dar prioridad a la libertad de información cuando prima el interés general y se trata de información veraz, como se señala en el Auto dictado el 18 de mayo de 2009 en el fundamento jurídico tercero[56]. Aunque en este auto, en contraposición, no existe prevalencia del derecho a la información al producirse una intromisión en el derecho a la autodeterminación informativa. En el supuesto se producía un tratamiento no consentido por la publicación de datos personales de médicos y farmacéuticos que respondía al objetivo de provocar un mayor impacto por el abuso en la prescripción de antibióticos y los perjuicios para la salud por estos profesionales (indicando que podría haberse publicado tal información sin hacer referencia a la identidad de los profesionales aunque esta información se hubiese recogido de fuentes públicas como los Colegios de médicos).

Por último, cabe señalar que el derecho al olvido guarda especial relación con nuestro tema, ya que los datos de posicionamiento contienen información personal que debe poder ocultarse o eliminarse de la vista de terceros. Un ejemplo de ello son las imágenes que contienen metadatos sobre la ubicación, fecha en la que fue tomada, dispositivo, entre otro tipo de datos.

1.4.- Derecho al anonimato

Este derecho ampliaría el derecho al secreto de las comunicaciones, en específico, las que se realizan a través de las TIC. Vendría a suponer la opción a que seamos anónimos cuando se haga uso de internet sin que, por ejemplo, nuestro buscador obtenga nuestra dirección IP desde donde realizamos la búsqueda. Además no existiría un tratamiento de datos en sí porque estos no quedarían registrados ni serían conservados. Tiene su paralelismo en la ocultación del número de teléfono en el artículo

[55] http://www.abc.es/tecnologia/redes/20140709/abci-derecho-olvido-google-201407091214.html última consulta: 21.06.2017.
[56] RJ 2009/155.

47.1.m) de la Ley General de Telecomunicaciones (en adelante LGT[57]) por el que los usuarios tienen el "*derecho a impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere o la presentación de la identificación de su línea al usuario que le realice una llamada*". La única vía más accesible que existe para navegar de forma anónima es mediante Tor Browser[58] que no viene a ser del todo sencilla para los usuarios.

2.- La protección de datos personales donde están incluidos los datos de localización

Como ya veníamos adelantando, la intromisión en la privacidad de los individuos motiva el análisis de ciertos aspectos, entre ellos, el consentimiento del interesado, qué es lo que implica el tratamiento de datos y los conflictos que pueden surgir cuando se ceden estos datos.

Debemos tener en cuenta, en cuanto a protección de datos se refiere, que existe un ente, la Agencia Española de Protección (AEPD) que se encarga de velar por el cumplimiento de la normativa sobre protección de datos y, entre otras cosas, nos ofrece información sobre este tema[59]. Es una autoridad estatal de derecho público que posee personalidad jurídica propia y plena capacidad pública y privada, la misma actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Este ente fue creado a partir del Real Decreto 428/1993, de 26 de marzo, por el que se aprobó su Estatuto en el que en su artículo 3 se remite a las funciones que se enumeran en el artículo 37 de la LOPD. Desde el plano de los afectados debe encargarse de informar acerca de los derechos que les asisten a estos en lo referido al tratamiento automatizado de sus datos personales. También deberá atender a las peticiones de los afectados y resolver las reclamaciones que le formulen. Asimismo deberá realizar

[57] Ley 9/2013, de 9 de mayo, General de Telecomunicaciones.
[58] http://computerhoy.com/noticias/software/navegacion-privada-tor-que-es-como-funciona-41301 última consulta: 21.06.2017.
[59] La Agencia Española de Protección de datos en su página web oficial ofrece un glosario donde podemos consultar de forma rápida todos los conceptos relacionados https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/preguntas_frecuentes/glosario/index-ides-idphp.php última consulta: 21.06.2017.

memorias anuales para analizar los problemas con la protección de datos o analizar que tendencias legislativas, jurisprudenciales y doctrinales existen en otros países, ya que está en evolución con las nuevas tecnologías de la información. Por todo ello, su función es clave en esta materia.

2.1.- Conceptos clave

Para poder profundizar en las cuestiones relativas a la protección de datos debemos partir de una serie de conceptos como el de *datos de carácter personal*. Establece la Ley Orgánica de Protección de Datos (en adelante LOPD[60]) en el artículo 3.a) que será "*cualquier información concerniente a personas físicas identificadas o identificables*". En este marco encuadramos lo que refiere a *datos de localización* para los que se ofrece una definición en el artículo 2 de la Directiva 2002/58/CE[61] entendiéndose "*cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones geográficas disponible para el público*".

En el Dictamen 4/2007[62] sobre el concepto de datos personales adoptado el 20 de junio se refleja desde varias perspectivas el concepto de dato: respecto a su naturaleza "*incluye todo tipo de afirmaciones sobre una persona*", es decir, "*abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas»"*. Desde el punto de vista del contenido integra cualquier dato que proporcione información independientemente de la clase que sea la misma incluyendo así información sensible (artículo 8 de la Directiva que en nuestra LOPD se regula en el artículo 7) como otra información que no tenga este carácter[63]. Desde el punto de vista del formato o soporte

[60] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[61] 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). Su precedente fue la Directiva 95/46/CE de 24 de octubre.
[62] Dictamen 4/2007 sobre el concepto de datos personales adoptado el 20 de junio por el Grupo de Trabajo del artículo 29.
[63] Señala que "el término «datos personales» comprende la información relativa a la vida privada y familiar del individuo *stricto sensu*, pero también la información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o

se incluye cualquier forma –alfabética, numérica, gráfica, fotográfica o sonora- por lo que también se entiende incluida en el ámbito del tratamiento automático de datos.

2.2.- Consentimiento del interesado

Partiendo de estos conceptos, como son especialmente sensibles en relación al derecho al honor y a la intimidad personal, entre las cuestiones que debemos analizar se encuentra el consentimiento en relación al tratamiento de datos. Es decir, si el interesado acepta y es plenamente consciente de todo lo que implica el tratamiento y conservación de esta información sobre su persona no existiría mayor discusión. Cuando este consentimiento es prestado sin que sea debidamente informado y recabado en las formas que se prevén para ello no podría darse el tratamiento y si esto ocurriese sería constitutivo de una infracción. Se fundamenta en la privacidad como libertad individual la que otorga el poder para decidir si se permite que los datos sean utilizados por un tercero, tanto si estos datos de ubicación son públicos o son privados. Para ello es fundamental determinar si el consentimiento es válido atendiendo a lo que lo caracteriza.

En primer lugar, la capacidad requerida –para poder consentir y por ello aceptar esta relación jurídica cuyo objeto es el tratamiento de sus datos personales– es la general[64]. Esta capacidad general se contiene en el artículo 322 del Código Civil por la que se entiende capaz a todo mayor de edad siempre y cuando no concurran causas de incapacitación que se regulan en el artículo 200 del Código Civil.

En la definición que se contempla en el primer texto con carácter europeo[65] en esta materia obtenemos las notas esenciales del consentimiento: "*toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el*

social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.)".

[64] APARICIO SALOM, J., Elemento formal…, ob. cit. p. 143.

[65] Nos referimos a 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.

tratamiento de datos personales que le conciernan"[66] y completando con lo establecido en el artículo 6.1 de la LOPD por el que se "*requerirá el consentimiento inequívoco del afectado*" obtenemos el consentimiento que se considera válido. Por tanto, debe ser *libre*, es decir, sin ningún tipo de intervención, coacción, ni vicio alguno en la prestación del mismo; *específico*, que sea referido a un determinado tratamiento y finalidad; que sea *informado* ya que el interesado debe conocer previamente para que se van a utilizar sus datos, y no menos importante, debe ser *inequívoco* en el sentido de que sea expresado sin dar lugar a dudas. En relación a este último punto, la forma de prestar el consentimiento no es determinante para establecer la relación, ya que no es requisito la formalización del acuerdo de voluntades de una forma específica (no va a requerir escritura pública por ejemplo)[67].

Desde nuestro punto de vista, debería establecerse que el consentimiento siempre sea expreso ya que en conexión con las notas esenciales del propio consentimiento, la exigencia de que sea inequívoco podría verse mermada si se admite el consentimiento presunto o tácito (que se basa en la deducción del comportamiento del usuario). Ante esta cuestión el Grupo de Trabajo del artículo 29[68] en el Dictamen adoptado[69] establece que para que el consentimiento sea otorgado de forma inequívoca no debe existir "*ninguna duda sobre la intención del interesado […] en otras palabras, la manifestación mediante la cual el interesado consiente no debe dejar lugar a ningún equívoco sobre su intención. Si existe una duda razonable sobre la intención de la persona se producirá una situación equívoca*"[70]. Por tanto, es necesario que el consentimiento sea válido para no conculcar la legalidad. Por su parte la AEPD y nuestro legislador admite el consentimiento implícito, ya que sólo se exige la forma

[66] Artículo 2.h) de la Directiva 95/46/CE que es el mismo concepto que establece el artículo 3.h) de la Ley Orgánica de Protección de Datos de Carácter Personal, la única diferencia es que este último añade la nota de *inequívoca* como manifestación de voluntad.
[67] APARICIO SALOM, J., Elemento formal…, ob. cit. pp. 149-153.
[68] El Grupo de trabajo referido fue creado en virtud del artículo 29 de la Directiva 95/46/CE y se trata de un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.
[69] Dictamen 15/2011 sobre la definición del consentimiento adoptado el 13 de julio de 2011.
[70] Aclaración que establece el Dictamen 15/2011 en la página 23 en relación al artículo 7.a) de la Directiva 95/46/CE.

expresa ante el tratamiento de datos especialmente protegidos (artículo 7 LOPD), y no establece nada para el resto de tratamientos. Por tanto, el consentimiento al que se refiere el artículo 6.1 LOPD no podemos determinar que sea el expreso[71].

Siguiendo esta línea, la cuestión acerca de la admisión del consentimiento tácito o presunto no es tan relevante si consideramos cómo se obtienen y conservan los medios de prueba que sirven para acreditar que se ha obtenido este consentimiento independientemente de su forma. Dado que la declaración de voluntad no se suele recoger por escrito tratándose de servicios que se realizan de manera virtual, motivó a que en la Sentencia del Tribunal Supremo de 15 de julio de 2010 en el fundamento jurídico noveno[72] se estimase la impugnación del artículo 18 del RLOPD (artículo que fue posteriormente anulado) sobre la acreditación del cumplimiento del deber de información que exigía la conservación del soporte en el que conste este cumplimiento[73]. La anulación de este artículo no derivaba del hecho de que el consentimiento explícito sea imposible de ser prestado de forma digital, sino que a raíz de admisión de la libertad de forma -por parte del legislador- resultaba incompatible con la anterior exigencia del artículo[74]. Asimismo, como indica la Sentencia de la Audiencia Nacional de 15 de octubre de 2012 (fundamento jurídico tercero[75]) el encargado del tratamiento de datos va a ser el que deba acreditar el consentimiento del afectado, ya que solo el consentimiento justifica o legitima el tratamiento y aquí será donde entren en juego los medios de prueba admitidos en Derecho para determinar sin incertidumbres que tal voluntad ha sido manifestada.

[71] APARICIO SALOM, J., Elemento formal…, ob. cit. p. 153.
[72] RJ 2010/6271.
[73] APARICIO SALOM, J., Elemento formal…, ob. cit. pp. 153-154.
[74] El Grupo de Trabajo del artículo 29 en el Dictamen 15/2011 expresa que "En el entorno electrónico, el consentimiento explícito puede darse mediante firmas electrónicas o digitales. También puede darse pulsando botones según el contexto, enviando mensajes electrónicos de confirmación, pinchando en iconos, etc. Los procedimientos que implican una acción afirmativa de la persona se confirman en el considerando 17 de la Directiva sobre privacidad, que establece: «El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio *web* en Internet»".
[75] RJ 2012/342116.

2.3.- Tratamiento de datos. Elementos formales y subjetivos

Para que pueda darse el tratamiento es requisito esencial que el sujeto preste su consentimiento y como señala BATUECAS CALETRÍO se comprende en este tratamiento "*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*"[76]. Es decir, debe ser el usuario el que opte por autorizar el tratamiento de los datos de posicionamiento y aquí también se incluye la posible utilización por un tercero. Un concepto más amplio y preciso integra "*cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción*"[77].

Será siempre necesario el consentimiento[78] del titular de los datos personales y cuando este se opone o no expresa su consentimiento de la forma en la que vimos en el apartado anterior es cuando existe una infracción porque se estaría llevando a cabo una actuación que va en contra de la voluntad del interesado. Esto conecta con lo que se entiende por tratamiento legítimo por lo que estaremos a lo dispuesto en los principios generales del artículo 12 del Reglamento de desarrollo de la LOPD[79] que pueden resumirse de la siguiente forma:

a) Como regla general, para el tratamiento de datos, el responsable debe recabar el consentimiento del interesado, salvo que la ley disponga otra cosa.
b) Este consentimiento va a ser referido a un tratamiento o serie de tratamientos concretos (alcance del consentimiento).

[76] BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015, p. 57. En relación con la Sentencia del TC 254/1993, de 20 de julio.
[77] Artículo 2.b) de la Directiva 95/46/CE.
[78] A modo de matización, en cuanto a tratamiento de datos podrá efectuarse sin consentimiento cuando se trate de una institución pública que los necesite como puede ser la Hacienda Pública y para casos en los que la propia Ley establece el deber de soportar el tratamiento al afectado.
[79] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

c) Existe un deber de información al interesado del tratamiento o tratamientos que se llevarán a cabo, indicando de forma inequívoca el objeto y finalidad de los mismos. Se prevé que si no se cumple con este requisito el consentimiento es nulo de pleno derecho. Este deber también es un derecho del afectado por el tratamiento que debe relacionarse con lo dispuesto en el artículo 5 de la LOPD.
d) Tendrá la carga de la prueba el responsable del tratamiento respecto de la existencia de dicho consentimiento.

Asimismo, como regla general, será necesario el consentimiento para el tratamiento y también para la cesión de datos personales del interesado como dispone el artículo 10 del RLOPD que establece los supuestos que legitiman dicho tratamiento o cesión. Añadiendo, en su apartado segundo, una serie de supuestos en los que es posible el tratamiento o cesión sin necesidad de consentimiento[80]. En relación a la geolocalización, el tratamiento tiene su justificación en la prestación del propio servicio, pero cuando nos referimos a la conservación, la utilización e incluso la difusión pueden estar excediendo de lo permitido, ya que el responsable, en principio, no necesita esta información a largo plazo. Si esto ocurriese sin el consentimiento muy probablemente existiría un tratamiento indebido de datos cuya consecuencia es la infracción. Debemos diferenciar este hecho, pues no se trata de un incumplimiento del negocio jurídico como contrato para la prestación de este servicio.

En cuanto al momento en que debe recabarse el consentimiento será previamente al uso de la aplicación atendiendo al artículo 16 del RLOPD en relación con el art. 48.2.c) de la LGT. Y a este respecto el Grupo de Trabajo del artículo 29 se ha decantado porque estos servicios de geolocalización deban estar desactivados de fabrica o desde un inicio para que el usuario consienta "*gradualmente la activación de aplicaciones*

[80] Supuestos que no trataremos porque se basan en que lo autorice una norma jurídica junto con el interés del responsable del tratamiento; aquellos supuestos en los que es necesario para el cumplimiento de un deber o cuando se trate de datos recogidos para funciones de las Administraciones públicas, entre otros supuestos que recoge el artículo 10.2 RLOPD.

específicas"[81]. Esto no es siempre así ya que en la mayoría de dispositivos se alienta al usuario a que active la geolocalización.

Una vez establecido el inicio a partir del cual se van a tratar los datos, la conservación es el siguiente punto y sobre esta cuestión la Ley de conservación de datos[82] en su artículo 5 establece la facultad para que las operadoras conserven los datos de los usuarios, entre ellos los de localización, el problema es que no son operadoras las empresas que tienen estos datos normalmente, sino Google para Android[83], que exige asociar una cuenta de Gmail en los dispositivos, Apple en iOS o Microsoft en los teléfonos con sistema Windows Phone. A modo de ejemplo, cuando por razones de emergencia se necesita conocer la ubicación de una persona para prestarle auxilio, dado que no se prevé en la legislación actual que estas empresas tengan la obligación de ceder estos datos, los plazos se alargan por tener que solicitar previamente la cesión de los mismos. Además, en la Ley de Enjuiciamiento Criminal no existe una norma expresa para que los jueces ordenen la obtención de estos datos por estas compañías (se señala en el fundamento jurídico primero de la Sentencia del Tribunal Supremo de 7 de julio de 2016[84] en la que se cuestiona si la utilización de dispositivos GPS por el que se recaben datos de localización supone una intromisión lícita en el ámbito de una investigación criminal). En cambio sí se prevé en el caso de operadoras de telefonía por lo que nos lleva al siguiente conflicto, ya que la georreferenciación *"procede de sistemas de satélites cuyos servicios Google o Apple arriendan, pero cuya propiedad es del gobierno de Estados Unidos u otras instituciones de carácter internacional, pues se trata de tecnología de origen militar. De ahí que existan posibles problemas de jurisdicción y de confidencialidad a la hora de pedir estos datos*[85]".

[81] En la página 15 del Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes adoptado el 16 de mayo de 2011.
[82] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
[83] Android: "Es un sistema operativo móvil basado en Linux, que junto con aplicaciones middleware está enfocado para ser utilizado en dispositivos móviles como teléfonos inteligentes, tabletas, GoogleTV y otros dispositivos. Es desarrollado por la Open Handset Alliance, la cual es liderada por Google". En http://www.movieonmovil.com/glosario-de-celulares.html#S última consulta: 21.06.2017.
[84] RJ 2016/3786.
[85] Extracto de la noticia http://www.eldiario.es/turing/smartphones-gps-rescate_0_350315050.html última consulta: 21.06.2017.

En lo que refiere al aspecto subjetivo del tratamiento de datos, cabe distinguir a una serie de sujetos, entre ellos al responsable y al encargado del tratamiento. El responsable[86] va a ser el que se encargue de establecer la finalidad y los medios del tratamiento y el encargado[87] va a ser el que efectúe el tratamiento en sí y del modo en que le indique el responsable. Sobre esta cuestión, el Grupo de Trabajo del artículo 29 en el Dictamen 1/2010[88] indica que sobre el responsable del tratamiento recaen una serie de obligaciones entre las que se encuentran la notificación y controles previos de dicho tratamiento y además de la posible responsabilidad ante un tratamiento ilícito de datos. Es decir, va a ser frente al responsable ante quién se dirijan los afectados para ejercer sus derechos por ser el ente que "*ha decidido tratar datos personales para sus propios fines*"[89]. Genera dudas sobre quien va a ser el responsable cuando se comparte esta responsabilidad y cuando además se le otorga cierta autonomía al encargado del tratamiento, complicando aún más la determinación del mismo cuando el responsable se ha establecido en el territorio de varios Estados miembros[90] y más aún fuera de la Unión Europea. A este respecto deben cumplirse siempre con las obligaciones previstas en el ordenamiento jurídico del país en concreto tal y como establece el artículo 4.1.a) de la Directiva 95/46/CE y atenderse a los artículos 33 y siguientes de la LOPD.

De cara al sujeto afectado por el tratamiento, éste puede conocer quién es el responsable del tratamiento acudiendo al Registro General de Protección de Datos cuya función es la de velar por la publicidad de los tratamientos de datos y de la inscripción de ficheros independientemente de la titularidad, ya sea privada o pública.

---

[86] Definición en el art. 3.d) de la LOPD que en la Directiva 95/46/CE en el art. 2.d) se explica de forma más completa por la que responsable del tratamiento es "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario*". También se denomina responsable del fichero.

[87] Misma definición en el art. 3.g) de la LOPD y en el art. 2.e) se establece que el encargado del tratamiento es "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

[88] Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» adoptado el 16 de febrero de 2010 por el Grupo de Trabajo del Artículo 29.

[89] En el Dictamen 1/2010, p. 5.

[90] APARICIO SALOM, J., Elemento subjetivo de la relación: las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 69.

Otra distinción que debemos hacer es entre responsable del fichero y responsable del tratamiento, ya que del artículo 3.d) LOPD se puede inducir que se refiere a lo mismo[91]. Son conceptos que no deben confundirse a criterio de la AEPD y como refleja la sentencia de la Audiencia Nacional de 16 de octubre de 2003 (fundamento jurídico tercero[92]). Aunque considera APARICIO SALOM que es una distinción forzada y sobre la que el Grupo de Trabajo del artículo 29 se remite a la Directiva 95/46[93] que establece como concepto comunitario el de *responsable del tratamiento,* añadiendo que no está sujeto a variaciones en las legislaciones de los Estados miembro.

Por otro lado, el encargado, que como veníamos señalando, es el ente que no ha determinado unos fines para los datos personales, pero que tiene un interés directo en el tratamiento. Dado que no establece que medios y fines para el tratamiento se van a dar, tampoco va a incurrir en posibles responsabilidades. Es una posición un tanto "cómoda" por la que efectuará un tratamiento de datos pero no se le atribuirán las consecuencias negativas del mismo. Al igual que como se señala en el artículo 20 del RLOPD en su apartado primero, no se considerará comunicación de datos si se trata de la prestación de un servicio al responsable. En cambio, si el acceso a los datos tiene como fin crear *"un nuevo vínculo"*, en este caso se considerará tercero y estaría estableciendo sus propios fines y medios, por tanto, pudiendo incurrir en responsabilidad por un tratamiento de datos inadecuado.

Los terceros –que no son encargados- tienen un interés legítimo (art. 7.f directiva 95/46), es decir, están legitimados para tratar datos personales para la satisfacción de dicho "*interés legítimo, singular y propio, pero adecuando los fines y medios del tratamiento de datos a lo que determina otra entidad, que será responsable*

[91] APARICIO SALOM, J., Elemento subjetivo de la relación: las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 71-72.
[92] RJ 2004/271.
[93] Esta Directiva será derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En este reglamento se indica en su artículo 99.2 que solo será aplicable a partir del 25 de mayo de 2018 por lo que seguimos atendiendo a la Directiva 95/46/CE.

de ese tratamiento"[94]. Ahora bien, debemos matizar que entre las obligaciones del responsable se encuentra la de impedir que terceros accedan de forma indebida a los datos personales (artículo 9 LOPD en relación a la seguridad de los datos) y el deber de secreto (artículo 10 LOPD). Por ello, si dicho responsable permite el acceso indebido a terceros se estaría incumpliendo estas obligaciones y entraríamos en la denominada cesión de datos que trataremos en el siguiente apartado.

Centrándonos en estas obligaciones de cara al responsable, de carácter material tenemos el respeto a la voluntad del interesado cuyo incumplimiento se considera infracción de la libertad del consentimiento. Sirve como medida de defensa de los afectados por el tratamiento de datos e incluye:

a) "*La recogida de datos en forma engañosa y fraudulenta*" que recoge el artículo 44.4.a) LOPD en relación al art. 4.7 LOPD.

b) El sometimiento del tratamiento de datos en contra de la voluntad del interesado o cuando se alteran los medios y finalidad de los mismos y no se informa debidamente (art. 44.3.b al igual que 44.4.b). Este último precepto incluye los supuestos del artículo 7.3 y 7.4 ya que de la geolocalización se pueden extraer datos, por ejemplo, acerca de creencias religiosas (encontrarse en actos o lugares de culto) y por ello constituye infracción si no se consiente de forma expresa[95].

c) El tratamiento se mantendrá mientras no revoque el consentimiento el interesado (derecho de cancelación del artículo 16 LOPD) o cuando se ejercite la oposición (artículo 34 del RLOPD) que es el derecho a que se deje de llevar a cabo el tratamiento o se cese en el mismo y en los supuestos que prevé el propio artículo y de la forma que establece el artículo 35 para su ejercicio. Cuando se impide o dificulta el ejercicio de estos derechos -cancelación y oposición- se considera infracción leve (44.2.e) LOPD). La infracción surge a raíz de una conducta en la que se pongan trabas a la hora de su

[94] APARICIO SALOM, J., Elemento subjetivo…, ob. cit. p. 79.

[95] Establece el apartado 7.3 y 4 LOPD: *"3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.*
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual".

ejercicio ya que el responsable puede poner requisitos o condiciones para que puedan ejercerse estos derechos que deberán estar justificadas.

d) Este impedimento u obstaculización (infracción grave art. 44.3.e) tiene relación con el derecho de acceso del artículo 15 de la LOPD que es el derecho a *"solicitar y obtener gratuitamente información de sus datos de carácter personales sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos*". Aunque se discuta la oportunidad de este derecho de acceso porque se presume que si el usuario ha aceptado el tratamiento conoce, por tanto, la información que se gestiona, lo cierto es que lo consideramos necesario, dado que si no conocemos en profundidad qué información es la que está tratando el responsable, no podremos ejercitar de forma adecuada el derecho de acceso, rectificación, cancelación y oposición (ARCO)[96].

Los derechos ARCO se regulan en los artículos 27 a 30 de la RLOPD en los que se indica que se ejercitará la acción correspondiente mediante petición o solicitud dirigida al responsable para salvaguardar estos derechos. Se tendrá el plazo máximo de un mes para resolver la solicitud desde que se recibe (29.1). En el derecho de acceso se aplican también las reglas generales aplicables a cualquier derecho, entre ellas la prohibición del abuso[97], como señala la Sentencia del Tribunal Supremo de 26 de enero de 2010 (fundamento jurídico cuarto[98]) referida a la solicitud de acceso en un caso en que se presentó una reclamación ante la AEPD por el incumplimiento de este derecho cuando el solicitante disponía ya del acceso a los datos personales a través de un

[96] A la hora de solicitar esta información no siempre ha sido sencillo y prueba de ello es lo que le ocurrió al señor Malte Spitz que solicitó a su compañía de teléfonos alemana que le enviara todos los datos que había conservado sobre su persona. La compañía se negó y solo fue tras dos demandas cuando le envió dicha información cuyo formato no podía comprender por lo que contactó con una agencia de desvisualización de datos y combinaron estos datos con sus datos públicos (en redes sociales mayormente) y crearon un mapa. Este "diario digital" contenía una gran cantidad información: los sitios a los que viajaba, donde dormía (por la inactividad), que llamadas hacía, etc. El documento contenía información de 6 meses porque la Directiva de 2006/24/CE establecía que los Estados miembros tenían la obligación de conservar los datos personales por un tiempo que no fuese inferior a 6 meses ni superior a 2 años. En España la transposición de esta directiva dio lugar a la Ley 25/2007, de 18 de octubre, de conservación de datos que ya no se encuentra vigente. En el siguiente enlace Malte Spitz explica su caso https://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=es#t-492133 última consulta: 21.06.2017.

[97] APARICIO SALOM, J., Derechos y obligaciones de las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 298.

[98] RJ 2010/3154.

ordenador. Por tanto, no puede exigirse tampoco por parte del responsable otras vías para que facilite los datos si ya están en disposición del afectado.

Otra forma de garantía para los afectados se encuentra en el derecho "*a que se modifiquen los datos que resulten ser inexactos o incompletos*", es decir, el derecho de rectificación que se regula en el artículo 31 del RLOPD conjuntamente con el de cancelación cuyo ejercicio conlleva la supresión de "*los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo*". En cuanto a la solicitud de rectificación deberá indicar a que datos se refiere y a la corrección que deba realizarse (art. 32) basándose en el principio de calidad, a diferencia del derecho de cancelación, que se basa en la voluntad del interesado y en la libertad de revocación del consentimiento que hubiera otorgado[99]. Aunque la regla general es la libertad de revocación, algunas veces puede verse limitada a raíz del artículo 33.1 RLOPD que prevé la denegación de los derechos de rectificación y cancelación[100]. Hablamos de casos en los que el tratamiento está amparado en una obligación legal o en la ejecución de un contrato que haya sido libremente celebrado entre el responsable y el interesado.

Siguiendo con este análisis de las vías de protección de los interesados tenemos el derecho de oposición (al que hace referencia los artículos 6.4 y 30.4 LOPD y el artículo 35 RLOPD) que también se ejerce a través de solicitud al responsable y en síntesis es la negativa a que se continúe con el tratamiento por parte del responsable. Su origen viene del artículo 14 de la Directiva 95/46/CE el cual prevé que podrá hacerse en

[99] APARICIO SALOM, J., Derechos y obligaciones de las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 300.

[100] El artículo 33 RLOPD prevé los siguientes supuestos de denegación:
"*1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.*
2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre".

cualquier momento, por razones legítimas propias, siempre y cuando atendiendo a la legislación del Estado miembro y, además, que será sin gastos.

Se pueden distinguir dos casos: bien cuando se rechaza o manifiesta su oposición frente a unos usos concretos o finalidades concretas o bien cuando se realiza una oposición general al tratamiento. Respecto a los supuestos en que cabe oposición estaremos a lo dispuesto en el artículo 34 del RLOPD:

a) Cuando para el tratamiento no se necesite su consentimiento por concurrir un motivo legítimo y fundado "*referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario*".

b) "*Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial"* en relación al artículo 51 de esta Ley.

c) *"Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento".*

Estos derechos de acceso, rectificación, cancelación y oposición (ARCO) son derechos personalísimos y deben ser ejercidos por el propio afectado como indica el artículo 23 LOPD, aunque si fuera menor de edad o persona con la capacidad jurídica modificada judicialmente podrá su representante legal ejercitar estos derechos en su nombre. Asimismo, del artículo 24 en su apartado segundo y tercero se extrae el principio de gratuidad por lo que se entiende que el responsable no puede exigir, para el ejercicio de estos derechos, medios que supongan un coste desmedido o que sea a través del envío de cartas certificadas o el uso de servicios de telecomunicaciones de tarifación adicional[101].

Por último, debe regir el principio de acceso universal de forma que el afectado pueda realizar la comunicación al responsable por cualquier medio aunque no sea el concreto para el ejercicio de los derechos nombrados (el artículo 24.4 prevé que podrán utilizarse los servicios de atención al público o de reclamaciones previstos por el

[101] APARICIO SALOM, J., Derechos y obligaciones…, ob. cit. p. 307.

responsable del tratamiento). Esto es posible como bien establece el apartado 5 del propio artículo, por el que el responsable deberá atender a la solicitud de acceso, rectificación, cancelación u oposición ejercida aunque no hubiese utilizado la vía específica para dicha solicitud.

A la hora de ejercer estos derechos debe conocerse, como veníamos diciendo, la existencia de dicho tratamiento, los medios y el fin del mismo y la identidad del responsable. Para ello existe el Registro General de Protección de Datos donde podremos conocer esta información que es de consulta pública y gratuita (artículo 14 LOPD). Cuando el responsable del tratamiento no atiende a la solicitud efectuada por el afectado, este último podrá dirigirse a la AEPD por los siguientes motivos: (i) porque el responsable no haya contestado en el plazo de un mes desde la recepción de la solicitud; (ii) por haber denegado el acceso completamente (deberá documentarse con copia del escrito) o (iii) por no haber contestado satisfactoriamente a la petición de acceso (deberá también documentarse con copia del escrito)[102]. Aparte de esta función concreta de la AEPD, en el artículo 37 se enumeran toda una serie de funciones y es por eso que de oficio podrá también efectuar controles, de ahí que no solo sea el afectado *motu proprio* el que deba movilizarse para reaccionar frente a los incumplimientos del responsable.

El incumplimiento de estos derechos y en relación a las infracciones que prevé el artículo 44 LOPD conllevará la imposición de sanciones reguladas en el art. 45 por el que para las infracciones muy graves se prevén multas que pueden alcanzar hasta los 600.000€. En todo caso la cuantía atenderá al carácter de la infracción, el volumen de tratamientos realizados, los beneficios obtenidos, entre otros factores. A su vez, puede dar derecho a indemnización que se regula en el artículo 19 de la LOPD. Estas cuestiones no las analizaremos por desviarse de nuestro tema todo lo referido al régimen sancionador, pero podemos determinar que se pueden acudir a varias vías: a través de la AEPD cuyas resoluciones agotan la vía administrativa (art. 48.2 LOPD); a través de la vía civil y a través de la vía penal.

[102] https://sedeagpd.gob.es/sede-electronica-web/vistas/formReclamacionDerechos/previoReclamacionDerechos.jsf última consulta: 21.06.2017.

Por otro lado, es fundamental que tengamos en cuenta que el responsable tiene toda una serie de obligaciones que debe cumplir y que se establecen en el artículo 4 de la LOPD bajo la denominación de calidad de datos. Integra el principio de pertinencia de los datos; el deber de cancelación de los datos innecesarios (si una aplicación no necesita la ubicación para su funcionamiento no debería utilizarse); la adecuación del tratamiento a la finalidad autorizada; deber de actualización y rectificación; los deberes respecto de la organización del tratamiento; deberes éticos en la recogida de datos; el deber de notificar las fugas de información y el deber de secreto[103]. A su vez, se deduce también de este principio de calidad el hecho de que la información no debe conservarse por tiempo indefinido porque se estaría infringiendo este mismo principio (art. 4.5 párrafo segundo).

Sin separarnos de la dificultad que plantea el uso de los datos de georreferenciación de los usuarios, en este sentido, no resulta sencillo delimitar el régimen de responsabilidad en cuanto al tratamiento indebido de datos que deriven del uso de sistemas GPS, pues, en concreto, existe una pluralidad de sujetos que pueden ser responsables[104]. Partiendo de este tratamiento adecuado -ya mencionado- sólo podrán recogerse datos personales "*cuando sean adecuados, pertinentes y no excesivos*" completando con que "*no podrán usarse para finalidades incompatibles*", al igual que deberán ser "*exactos y puestos al día*" (art. 4.1, 2 y 3). Esto último es relevante ya que si son inexactos (total o parcialmente) o incompletos deben ser cancelados y, a su vez, sustituidos de oficio por aquellos datos rectificados o completados. Atendiendo a las finalidades sí que será compatible el tratamiento con fines estadísticos, históricos o científicos (art. 4.2 LOPD y el art. 9 RLOPD) limitando siempre la obtención de datos por medios fraudulentos, desleales o ilícitos (art. 4.7 LOPD).

En el reglamento que desarrolla esta ley, en su artículo 4 se establece qué ficheros o tratamientos están excluidos y son los "*realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas*". También

[103] APARICIO SALOM, J., Derechos y obligaciones…, ob. cit., p. 221.
[104] Como ya plantea BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización», *Derecho Privado y Constitución*, 2015, p. 77.

están excluidos los que se encuentren sometidos a la normativa sobre protección de materias clasificadas y los que estén relacionados con la investigación del terrorismo y otras formas graves de delincuencia organizada. Por tanto, cualquier otro tratamiento sí que estaría sometido tanto a la LOPD como a su reglamento de desarrollo.

Teniendo en consideración todo lo anterior, determinar quién es el responsable pasa por distinguir cuando el fabricante del dispositivo coincida además en ser el autor de la aplicación de geolocalización de cuando no sucede esto. Las posibilidades son las siguientes:

a) Cuando se trate del caso en que el fabricante solo lo es del hardware del dispositivo y no del software, aunque como bien señala BATUECAS CALETRÍO "*el hardware propicia el inicio del tratamiento de los datos personales*" es tan esencial para determinar que el fabricante del hardware pueda ser responsable jurídicamente del tratamiento de datos, ya que se trata de "*un mero prestador de acceso a servicios de telecomunicación*". Es decir, es el medio para que pueda instalarse el software que posibilita la obtención de estos datos.

b) Cuando el fabricante del hardware es también titular de la aplicación de geolocalización (ej. en el caso de los iPhone que Apple es fabricante tanto del hardware como del software iOS). En este caso sí queda claro que está "*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*"[105].

A su vez, podemos mencionar a un tercer responsable que es la operadora de telefonía que posibilita la transmisión de los datos. Aunque no es realmente su única función, pues va a obtener datos desde que se contrate la línea telefónica. Este momento lo podemos identificar con la introducción de la tarjeta SIM. Asimismo, en cada ocasión en que se de uso a la aplicación que recabará el tiempo que se utilice y para qué finalidad, también cuando se efectúe la contratación de la línea "*porque los necesita para el adecuado mantenimiento de la relación contractual […] y, a veces, con*

[105] BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015, p. 62.

intención comercial". En el último supuesto será la compañía telefónica la que ostente la titularidad del fichero que se creará para este destino convirtiéndose en la destinataria de su contenido y responsable de este.

Acerca de la problemática que conlleva la publicidad, la cual no es buscada por el afectado, por lo que deberá aceptar esta intención comercial, debemos tener presente el art. 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. A este respecto debe informarse adecuadamente para que el interesado consienta el envío de promociones, ya que si "*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*". También debe atenderse al artículo 30 de la LOPD en lo relativo al tratamiento con fines de publicidad. Esta última cuestión, es decir, la que tiene una finalidad comercial conecta más con la cesión de los datos personales que tratamos a continuación.

2.4.- Cesión de datos

Se considera comunicación o cesión de datos "*toda revelación de datos realizada a una persona distinta del interesado*" (art. 3.i) LOPD) y como forma de protección. A denominación de la directiva que lo entiende como "*terceros a quienes se comunican los datos*" (art. 2.f), es decir, a entes distintos que desarrollan un tratamiento específico. La protección de datos en estos casos pasa por un deber de información doble por parte del responsable pues requiere la previa información al afectado, al igual que la obligación de comunicarle al tercero las posibles solicitudes que haya efectuado el afectado –en relación al derecho de oposición de oposición y rectificación que puede consistir simplemente en la actualización de dicha información–[106]. De esta manera los terceros van a realizar el tratamiento de datos "sin preocuparse" de la serie de

[106] APARICIO SALOM, J., Elemento subjetivo de la relación: las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 83.

obligaciones y derechos que sí debe respetar el responsable. Dejarán de considerarse terceros si estos empiezan a determinar los medios y fines de dicho tratamiento.

2.5.- Aspectos problemáticos y posibles soluciones

Nos referiremos en este sub-epígrafe a una serie de cuestiones en relación a todo lo expuesto que pueden dar lugar a discusión y cierta problemática y trataremos de aportar algunas soluciones.

2.5.1.- En relación con la cesión de datos

Por lo que respecta a la cesión de datos, existe un "tercer" sujeto que no mencionábamos en el apartado anterior por no ser considerado ni responsable ni encargado, pero que conviene señalar. Nos referimos a las empresas de telecomunicaciones, pues estas se circunscriben a la prestación de un servicio para que el "mensaje" llegue al destinatario. Además, en muchas ocasiones no están vinculadas con el responsable a través de un contrato de servicios. Por ello, se entiende que estas tratan los datos de forma diferente como se expone en la Directiva[107]. El servicio de telecomunicaciones que nos interesa es el de internet y el de telefonía y en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones también se prevé en el artículo 41 la protección de datos por la que estos operadores[108] tienen el deber de adopción de medidas técnicas y de gestión que sean adecuadas para la preservación de la seguridad en la explotación de la red o prestación de servicios. Conecta, además, con una medida importante y es que en caso de violación de datos personales deberá el operador comunicarlo a la AEPD y si se tratara de casos aislados que afecten a uno o varios particulares, deberán notificárselo si pudiese afectar negativamente a la intimidad o a sus datos personales –sin dilaciones indebidas añade el artículo 41.3 de la LGT–.

[107] En el considerando 47 de la Directiva 95/46/CE se establece que "*cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio*".

[108] Nos referimos a operadores que explotan redes públicas de comunicaciones electrónicas o que prestan servicios de comunicaciones electrónicas disponibles al público, así como las redes públicas de comunicaciones que dan soporte a dispositivos de identificación y recopilación de datos.

Completando con el artículo 11, acerca de la comunicación de datos, se establece que dicha comunicación a un tercero solo podrá realizarse para fines concretos y mediando el consentimiento del interesado, que debe ser siempre previo. Esto último significa que no podrá darse la comunicación y posteriormente la obtención del consentimiento. Por ello, si dejamos a un lado las excepciones al consentimiento que están autorizadas por ley (por tratarse de datos que hayan sido recogidos en fuentes accesibles al público, etc.) lo cierto es que la cesión no es sino otra forma de tratamiento que requiere, a su vez, que sea informada para que pueda ser eficaz y cuyo incumplimiento prevé la consecuencia de la nulidad de forma directa (art. 11.3).

Por lo que refiere a las medidas de seguridad, aparte de las expuestas, referidas a los derechos de los afectados y las obligaciones y deberes del responsable, también se prevé algunas en la Ley General de Telecomunicaciones. En concreto, en el art. 43 se prevé una forma de protección de las comunicaciones exigiendo el cifrado para la información que es transmitida por redes de comunicaciones electrónicas[109]. El cifrado sirve para que un tercero no pueda escuchar o captar una comunicación entre un emisor y un receptor, pero esto no es siempre suficiente para salvaguardar nuestra privacidad. No es suficiente porque si hablamos de proteger nuestros datos personales incluidos los de la ubicación, el cifrado solo dará mayor protección en lo que refiere a mensajería –independientemente de las múltiples formas de comunicación (llamadas, correos electrónicos, whats, etc.)-. Por ello debemos preguntarnos y considerar la utilidad que tendría en esta materia la encriptación, pues serviría para que toda esta información que puede pasar por operadores y empresas que utilizan los servicios de las antenas de telefonía y satélites no pueda ser fácilmente decodificada.[110] En nuestra normativa no se

[109] El cifrado "es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de cifra a efectos de su control de acuerdo con la normativa vigente" (art. 41.2 de la Ley General de Telecomunicaciones).

[110] La encriptación se puede definir como "*la codificación de la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red" para que así solo "a través de un software de descodificación que conoce el autor de estos documentos encriptados es como se puede volver a decodificar la información*". http://www.larevistainformatica.com/que-es-encriptacion-informatica.htm última consulta: 21.06.2017.

exige que la información de ubicación sea encriptada, de ahí que pueda quedar expuesta frente a otros usuarios y este incumplimiento tiene como consecuencia la infracción del deber de secreto. Este deber, como obligación material, se regula en el artículo 10 LOPD e implica, precisamente que sea calificada esta acción como cesión de datos (no existe una distinción entre la vulneración del deber de secreto y la cesión de datos).

La importancia de las políticas de privacidad es clave, pues informan sobre cómo una determinada organización retiene, procesa y utiliza los datos del usuario. Muchas veces se acepta y no nos aseguramos de las condiciones que pueden que haya detrás de un intercambio de información de una compañía a otra. Recientemente Estados Unidos aprobó una ley[111] (S.J. Res.34) que permite a los proveedores de Internet vender a otras compañías -por ejemplo: publicistas- los datos de usuarios -entre estos datos se encuentra su localización- sin su consentimiento, lo cual solo demuestra la vulnerabilidad de nuestra información. En palabras del congresista John Lewis, que votó en contra de su aprobación, "*los datos de los usuarios pertenecen a los consumidores, no a los proveedores, y nunca deberían ser vendidos para el beneficio de las grandes operadoras*". Resulta evidente que dicha información resulta atractiva para muchas compañías como fuente de ingresos.

2.5.2.- En relación con los derechos ARCO

Cuando mencionábamos los derechos ARCO, si estos no son ejercitados, y en relación al consentimiento, se considera que el usuario tolera el tratamiento de datos; y esto puede producirse en casos en que existan variaciones en el tratamiento de las que, a su vez, deberá informar el responsable. Se discute, a su vez, si estos derechos están subordinados al derecho de acceso[112], discusión ya resuelta en favor de la independencia de estos derechos (hecho que se evidencia en que se regulan en artículos diferentes art. 15 y art. 16 de la LOPD). Una forma de protección para el usuario o más bien, de facilitarle esta vía de forma más inmediata consistiría en la posibilidad de un efectivo

[111] http://internacional.elpais.com/internacional/2017/03/28/estados_unidos/1490738196_593249.html última consulta: 21.06.2017.
[112] APARICIO SALOM, J., Derechos y obligaciones de las partes. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 299.

control pudiendo negar el acceso a la información (y que también sea eliminada de sus bases o servidores), así como la posibilidad de control y seguimiento de la misma. También el poder controlar el uso que otros puedan hacer de información de una persona de forma más efectiva. Ya no solo debemos quedarnos con la facultad de exclusión sino con el verdadero dominio de que información queremos que sea conocida, tratada o cedida pudiendo revocar en todo momento. Ya que las respuestas para el ejercicio de los derechos ARCO pueden demorarse por parte del responsable del tratamiento, dado que si este último no atiende a las solicitudes debe entonces dirigirse el afectado a la AEPD conseguir el cumplimiento de estos derechos.

En relación a lo anterior y en contraposición, podemos determinar que es más complejo el amparo del derecho a la intimidad porque precisamente podemos haber prestado nuestro consentimiento a la hora del uso de estos datos sin ser plenamente conscientes de los riesgos o simplemente no se nos ha informado adecuadamente. Por ello, el derecho a la privacidad es el que debe entrar en juego en estos casos como un verdadero mecanismo y no como una mera expectativa de control que puede tener cada persona a la hora de controlar su información. Esto podría desarrollarse a través de la configuración de las cuentas en redes sociales que contengan nuestra información estableciendo una forma de descargar nuestro fichero de datos que pueda ser comprensible para el usuario (idea que ya ha sido desarrollada por algunas redes como Twitter). A su vez, añadiendo la función de poder decidir que información queremos eliminar de sus servidores, ya que todos podemos eliminar contenido de nuestra cuenta pero sabemos que ha quedado almacenado por si queremos recuperarlo en algún momento. Lo mismo sucede cuando se elimina una cuenta que se da la opción de inactivarla para en un futuro volverla a utilizar.

2.5.3.- En relación con el derecho al anonimato

El derecho al anonimato que ya explicamos conviene advertir una forma de protección del mismo, que es cambiando la naturaleza de estos datos. Cuando definíamos los datos personales decíamos que son aquellos datos que se asocian a nuestra persona. En contraposición tenemos el concepto de *dato disociado*, que se

refiere al conjunto de datos que no permiten la identificación de un afectado o interesado. En nuestro caso, los datos de localización nos identifican, nos relacionan con un determinado dispositivo a un determinado lugar. Pues bien, cuando estos datos sufren del procedimiento de disociación (art. 3.f) LOPD) no podrán volver a su anterior estado de forma que ya no podrán volver a vincularse con un determinado afectado. Es una vía de protección a la que pueden acudir los usuarios y que además permite la comunicación de datos a terceros sin aplicar el artículo 11 de la LOPD cuando estos datos son previamente disociados. Por ello, va a beneficiar al cesionario la obtención de los ficheros sin convertirse entonces en responsable y sin asumir las obligaciones que sí tendría que asumir si pudiesen identificar a una persona.

Desde nuestra perspectiva esta opción es más efectiva que el denominado *data masking* o enmascaramiento de datos[113], que encubre los datos de forma selectiva de manera que van a ser similares a los de origen pero no completamente. Esto supone que se sustituirán algunos datos cuando los reales no son necesarios para así no tener información completa (suele utilizarse para ocultar el número de las cuentas bancarias).

2.5.4.- Otros aspectos problemáticos

Por si no resulta alarmante el volumen de información que cualquier dispositivo que integre esta tecnología puede almacenar y gestionar, puede acumularse aún más información cuando se combina con la compartida en redes sociales. Esto a veces sucede aunque no sea nuestra intención ni hayamos activado el GPS dado que nuestros teléfonos están constantemente conectándose a las antenas de telefonía. Además, todos estos datos que se recaban no solo se utilizan por las empresas y compañías privadas sino que las instituciones públicas también pueden requerirlos, como sucedió en Ucrania[114]. Lo que ocurrió fue que a solicitud del Gobierno las operadoras facilitaron estos datos de localización de todos los usuarios que se encontraban en un determinado lugar participando en una manifestación ilegal. Utilizando la identificación de los usuarios se envió un mensaje disuasorio a los ciudadanos para así paralizar los

[113] http://www.powerdata.es/enmascaramientode-datos última consulta: 21.06.2017.
[114] https://hipertextual.com/2014/01/gobierno-ucrania-sms-protestas última consulta: 21.06.2017.

disturbios producidos. Pero lo que ocurrió es que en este SMS se advertía a todos los ubicados en la zona, estuviesen o no movilizándose, que habían sido registrados precisamente como participantes en la manifestación. Por tanto, fue enviado incluso a personas que simplemente estaban en sus hogares y no en las calles. De esta forma, la geolocalización se utilizó para identificar y como medio de control de una población, esto refleja una de tantas situaciones a la que podemos vernos expuestos sin ser conscientes de estar vigilados y sin consentir la cesión de nuestros datos de ubicación.

2.5.4.1.- La ubicación en tiempo real y la conservación de los datos

Otra de las cuestiones a las que no nos referimos en cuanto a la enumeración de usos, pero que cabe destacar, es que, dada su popularidad, WhatsApp[115] ha lanzado la posibilidad de compartir nuestra ubicación a tiempo real[116]. Dicha utilidad estará desactivada por defecto atendiendo al criterio europeo –Dictamen grupo de trabajo del artículo 29-. Es una forma rápida y útil para que una persona en apuros envíe su ubicación si no tiene instalada una aplicación específica para emergencias, ya que las compañías que recaban estos datos no están obligadas a proporcionarlos aunque se trate de casos de urgencia[117], por ello, es el usuario el que debe enviar su localización o llamar a los teléfonos de indicados en la tarea. Es una vía bastante útil porque gran cantidad de usuarios tienen esta aplicación y pueden enviar su ubicación a familiares y amigos para que los socorran facilitando las labores a los servicios que deban encargarse de dar respuesta estas situaciones.

Aunque podamos pensar que queda a nuestra elección que se utilicen nuestros datos de ubicación por el simple hecho de descargar una aplicación lo cierto es que no es necesaria una aplicación adicional para que se obtengan datos personales constantes sobre nosotros en nuestros dispositivos. En concreto, en los terminales Android en el menú de ubicación podemos acceder a nuestro historial de ubicaciones de Google.

[115] WhatsApp es un servicio de mensajería para teléfonos inteligentes: https://www.whatsapp.com/?l=es
[116] Noticia de https://www.xataka.com/aplicaciones/whatsapp-y-la-localizacion-en-tiempo-real-de-tus-contactos-ya-sabemos-como-funcionara última consulta: 21.06.2017.
[117] Noticia referida a un caso en el que se solicitó a Google datos de geolocalización del usuario y dicha empresa tardó alrededor de 30 días para facilitarlos dificultando la búsqueda de esta persona http://www.eldiario.es/turing/smartphones-gps-rescate_0_350315050.html última consulta: 21.06.2017.

También integra la denominada *Actividad en la Web y en aplicaciones*, esta función almacena tus búsquedas y otras actividades que realices en el buscador, en Maps y en otros servicios de Google, incluida tu ubicación y otros datos asociados[118]. Por tanto, es la razón por la que se nos ofrecen anuncios tan personalizados y cercanos a nosotros, es decir, combinando la información de las búsquedas y de ubicación. Si se encuentra activado estos datos pueden guardarse desde todos los dispositivos en los que hayas iniciado sesión, aunque siempre puedes controlar y revisar tu actividad. A su vez, ofrece la posibilidad de compartir la ubicación en Google con un contacto en específico o en las redes sociales tu ubicación en tiempo real[119]. Respecto a dispositivos con iOS[120] también hacen un seguimiento de los mismos, incluso de tabletas, como señala LÓPEZ JIMÉNEZ y DITTMAR respecto a que entre los ficheros que almacenaban en su memoria interna estos dispositivos se incluía uno llamado "consolidated.db" integrado por datos de localizaciones de estos terminales. Entre los usos de este fichero se encuentra el poder "*servir de ayuda para la geolocalización de aplicaciones de aplicaciones relativas al mapeo de rutas o soluciones de navegación GPS*" y lo más importante es que si desactivaba la aplicación el fichero seguía recopilando datos de ubicación y estos *"se compilaban durante un tiempo estimado superior a un año … no sólo en el propio aparato (el teléfono o Tablet), sino que también acontecía en el ordenador con el que, en su caso, se realizaba la sincronización con iTunes*" [121].

Lo expuesto conecta con la conservación de datos, pues una vez que transcurren los plazos previstos legalmente deberán eliminarse aunque no se haya ejercitado el derecho de cancelación[122] siguiendo así el principio de calidad (art. 4 LOPD) por el que

[118] Descripción que aparece en cualquier dispositivo con sistema Android lo que nos lleva a plantearnos ¿qué otros datos asociados se almacenan y a los que tiene acceso Google?
[119] Ejemplo: probé en mi teléfono y pude ver mi historial de ubicación día por día desde 2012 hasta 2017 y no era consciente de que lo hubiese activado. Además está almacenado en la cuenta de Gmail en la que puedo acceder a los datos de las rutas seguidas y lugares visitados durante este tiempo cuando he tenido la ubicación activada y he utilizado Google Maps.
[120] iOS es el Sistema Operativo desarrollado por Apple y específico para iPhones: https://www.apple.com/es/ios/ios-10/ última consulta: 21.06.2017.
[121] LÓPEZ JIMÉNEZ, D. DITTMAR, E. C. "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital" en VALERO TORRIJOS, J. *La protección de los datos personales en internet ante la innovación tecnológica*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 536.
[122] ALMUZARA ALMAIDA, C. (coord.), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª edición, ed. Lex Nova, Valladolid, 2007, p. 316.

el responsable tiene la obligación de cancelación. Esto implica que deberán borrarse físicamente los datos y, como vemos en los dos supuestos anteriores, no se cumple. Si bien una serie de datos *"estrictamente necesarios"* son requeridos para mantener el tratamiento, obligaciones contractuales y responsabilidades el resto que no tengan este carácter sí que deben ser eliminados[123].

2.5.4.2.- La georreferenciación con fines de investigación

Asimismo, el uso de la georreferenciación no se ha quedado solo en lo expuesto, pues por su utilidad, ya en el plano jurídico y en lo referido al contexto de una investigación ya se venía aplicando. Se considera como una diligencia de investigación y hasta la Ley Orgánica 13/2015[124], no podía colocarse ninguna baliza o dispositivo GPS si interfería con los derechos fundamentales del investigado. Ahora esta reforma prevé la regulación de la "*utilización de dispositivos técnicos de seguimiento y localización*" aceptando la injerencia con los derechos fundamentales. En cuanto al alcance que puede tener respecto a los derechos de la personalidad, ha sido objeto de discusión, y uno de los casos más sonados fue el de Uzun contra Alemania en la Sentencia del Tribunal Europeo de Derechos Humanos de 2 septiembre de 2010[125] en la que el recurrente había sido participe de delitos que habían sido cometidos bajo una organización terrorista cuya gravedad sirvió de argumento –entre otros- para establecer un juicio de proporción y valor. Se determinó que la instalación del dispositivo en su vehículo no interfería en su domicilio ni directamente sobre su persona. Por tanto, se entendió que dicha medida fue adecuada y no existía vulneración del artículo 8 del Convenio para proteger los Derechos Humanos y de las libertades fundamentales[126]. En contraposición, si se instalase en la propia persona vulneraría su derecho a la intimidad y en nuestra opinión no sería para nada efectivo a la hora de investigar porque calcularía sus movimientos dado que es consciente de que está siendo vigilado.

[123] ALMUZARA ALMAIDA, C. (coord.), *Estudio práctico…,* ob. cit., p.316.
[124] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.
[125] RJ 2010/301139.
[126] REYES LÓPEZ, J.I. «Los dispositivos técnicos de geolocalización. Régimen Jurídico a partir de la L.O. 13/2015». *Revista Aranzadi Doctrinal* núm. 4, Ed. Aranzadi, Cizur Menor, 2016. p.1.

2.5.4.3.- La geolocalización en el ámbito laboral

En el ámbito laboral se prevé que el empleador pueda adoptar "*las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adaptación y aplicación la consideración debida a su dignidad…*"; de esta manera regula el artículo 20.3 del Estatuto de los Trabajadores las formas de comprobación del trabajo que efectúan los empleados[127]. Por ello, en este ámbito también se ha aplicado la geolocalización como medida de control de los trabajadores lo que ha conllevado intromisiones ilegítimas en algunas ocasiones. Sobre todo se ha puesto de manifiesto cuando la prestación de servicios se lleva a cabo fuera del lugar de trabajo que también se justifica en el precepto citado y sobre lo que la doctrina del Tribunal Constitucional se decanta por afirmar que el contrato de trabajo no debe implicar la privación de derechos fundamentales al igual que la libertad de empresa del artículo 38 de la Constitución no legitima estas prácticas respecto de los trabajadores[128]. Deberá por tanto considerarse la oportunidad y atender a los fines de estas medidas de control por parte de los empresarios frente a los trabajadores.

2.5.4.4.- La geolocalización para la protección de menores

Por lo que refiere su uso en menores de edad conlleva a que afirmemos que su vulnerabilidad es aún mayor porque no están sensibilizados acerca de los riesgos. A los nativos digitales no les afecta verse expuestos de la misma forma que a los no nativos, pues parte de su concepción de sí mismos es como se muestran en las redes (se crean su status)[129]. Por ello deben analizarse ciertas cuestiones, respecto a su consentimiento no se prevé nada al respecto en la Directiva remitiéndose a la regulación que establezca cada Estado miembro, de ahí que en el dictamen emitido por el Grupo de Trabajo del artículo 29 critique este hecho ya que no reconoce una protección de forma específica

[127] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
[128] FERNÁNDEZ GARCÍA, A., «Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial», revista doctrinal Aranzadi social núm. 17/2010, Ed. Aranzadi, Cizur Menor, 2010, p. 2.
[129] No puede negarse el hecho de que los menores no tienen el mismo concepto de intimidad que tiene un adulto http://www.lavanguardia.com/tecnologia/20110709/54183271120/las-redes-sociales-hacen-perder-el-pudor.html última consulta: 21.06.2017.

para los menores de edad[130]. En nuestro país se prevé en el artículo 13 del RLOPD que podrán prestar su consentimiento los mayores de 14 años, de ahí que si tienen una edad inferior se necesitará el consentimiento de sus padres o tutores e independientemente de la edad cuando se necesitará la asistencia de los titulares de la patria potestad o tutela cuando se exija por Ley. Asimismo, en el reciente Reglamento europeo[131] se establece que el consentimiento es lícito si es prestado por un mayor de 16 años (artículo 8), aunque se prevé que se fijen edades inferiores por los estados miembros. Consideramos que con 14 años no se tiene la madurez suficiente ni la comprensión de lo que supone el tratamiento de datos por lo que elevar esta edad a la dispuesta en el reglamento puede resultar más protector para los menores.

Resulta además, contradictorio el hecho de que a la hora de celebrar un contrato –para adquirir un smartphone por ejemplo- por parte de un menor el mismo pueda anularse porque la capacidad que se exige para prestar su consentimiento en la contratación no es la misma que para el consentimiento del tratamiento de datos. La primera deriva de la capacidad general del artículo 1263.1º del Código Civil por la que si no cuenta con el consentimiento de sus padres no podría contratar, pero si sería válido el consentimiento prestado para el tratamiento[132]. Esta última afirmación es lo que considera BATUECAS CALETRÍO, pero desde nuestro punto de vista la compra de un dispositivo móvil puede considerarse habitual cuando se superan los 14 años, edad a partir de la cual es cuando los psicólogos consideran apropiado su uso y no antes[133].

[130] APARICIO SALOM, J., Elemento formal. Constitución del tratamiento. En *Estudio sobre la Protección de Datos*, 4ª edición, Ed. Aranzadi, Cizur Menor, 2013, p. 143.
[131] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
[132] BATUECAS CALETRÍO, A. «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015, p. 68.
[133] http://silviaalava.com/los-ninos-no-necesitan-un-telefono-movil-colaboracion-con-el-diario-el-mundo/ última consulta: 21.06.2017.

IV.- CONCLUSIONES

Acerca de todo lo expuesto podemos extraer las siguientes conclusiones:

I. Hemos visto como a través de la georreferenciación se obtienen datos personales y no únicamente los datos de ubicación, de ahí que podamos conocer lo relativo a la identidad y localización de los usuarios junto con otros datos que recogen nuestros smartphones que nos acompañan diariamente y han pasado a convertirse en rastreadores personales. Es por ello que no solo se conoce dónde estamos en un momento determinado, sino los sitios que frecuentamos, intereses y gustos personales, e incluso nuestros contactos más cercanos. Por si no resulta alarmante el volumen de información que cualquier dispositivo que integre esta tecnología puede almacenar y gestionar, puede acumularse aún más información cuando se combina con la compartida en redes sociales. Esto a veces sucede aunque no sea nuestra intención ni hayamos activado el GPS dado que nuestros teléfonos están constantemente conectándose a las antenas de telefonía.

II. Aunque nuestro ordenamiento jurídico ofrezca protección a los usuarios y articule los mecanismos necesarios cuando se traspasen los límites de la legalidad, en el uso de los datos de ubicación, desde nuestro punto de vista, los ciudadanos también deben cuidar la utilización de las TICs. Pues los usuarios cada vez dominan más los dispositivos, lo que permite que tengan un acceso más sencillo a la información que necesitan conocer. A raíz de ello, también deben actuar con diligencia pues tenemos la responsabilidad de protegernos de esta monitorización constante prestando nuestro consentimiento de forma consciente e informada, comprobando todo lo que supone el tratamiento de datos personales. En definitiva, todos dejamos una huella digital y debemos tener más consciencia de que cualquier actividad realizada deja rastro y esto puede utilizarse para fines que no deseamos.

III. El punto anterior debe ser matizado, ya que la información en bastantes ocasiones no es clara, sino difusa, de difícil acceso a través de los dispositivos y a veces

contradictoria (promueve su utilización argumentado un mayor aprovechamiento pero no advierte de las posibles consecuencias). Por ello, debe optarse siempre por ofrecer mayor claridad, sencillez y accesibilidad de la información que debe estar a disposición de cualquier usuario.

IV. Partiendo, a su vez, del análisis del derecho a la intimidad nos lleva a señalar que es necesario un efectivo control de la información en un sentido positivo y la exclusión de terceros y prohibición de la divulgación en un sentido negativo. Estas dos últimas ideas tienen su conexión directa con las políticas de privacidad tanto para ofrecer una mejor información al usuario como una vía de control autónoma de los datos que gestiona el responsable del tratamiento.

V. La normativa actual debe seguir progresando para llegar a ser aún más específica y garantista, añadiendo otras formas de seguridad como a través de la encriptación de la información de forma que no sea accesible a las compañías privadas ni puedan tener acceso a los programas de decodificación específicos para los usuarios. Es decir, la introducción de programas de encriptación personalizados para cada usuario con su propia codificación. Otra de las vías que mencionábamos para la protección de los usuarios es el enmascaramiento de datos de forma que se sustituyan algunos de los datos personales de manera selectiva para no poder identificar al afectado. En definitiva, debe apostarse por ofrecer todas las garantías que posibiliten el ejercicio de un control sobre el uso y destino de los datos, que a su vez, permita saber, quién, dónde, cuándo y para qué se han obtenido y registrado datos que conciernen a los afectados. Con el objetivo de poder hacer valer sus derechos los propios usuarios en caso de que sea necesario.

V.- JURISPRUDENCIA CONSULTADA

Tribunal Europeo de Derechos Humanos

STEDH de 2 de septiembre de 2010 (RJ 2010/301139)

Tribunal de Justicia de la Unión Europea

STJUE de 13 de mayo de 2014 (RJ 2014/85)

Tribunal Constitucional

STC de 2 de diciembre de 1988 (RJ 1988/231)

STC de 12 de noviembre de 1990 (RJ 1990/171)

STC de 20 de julio de 1993 (RJ 1993/254)

STC de 30 de noviembre de 2000 (RJ 2000/292)

STC de 28 de enero de 2003 (RJ 2003/14)

ATC de 18 de mayo de 2009 (RJ 2009/155)

Tribunal Supremo

STS de 15 de julio de 2010 (RJ 2010/6271)

STS de 26 de enero de 2010 (RJ 2010/3154)

STS de 7 de julio de 2016 (RJ 2016/3786)

Audiencia Nacional

SAN de 16 de octubre de 2003 (RJ 2004/271)

SAN de 15 de octubre de 2012 (RJ 2012/342116)

VI.- BIBLIOGRAFÍA

ALMUZARA ALMAIDA, C. (coord.), *Estudio práctico sobre la protección de datos de carácter personal*, 2ª edición, Ed. Lex Nova, Valladolid, 2007.

APARICIO SALOM, J., *Estudio sobre la Protección de Datos*. Ed. Aranzadi, Cizur Menor, 2013.

BATUECAS CALETRÍO, A., «Intimidad personal, protección de datos personales y geolocalización». *Derecho Privado y Constitución*, 2015.

BELTRÁN LÓPEZ, G., «La geolocalización social». *Polígonos, Revista de geografía*, núm. 27, 2015.

BIURRUN ABAD, F.J., «Pokemon Go y su impacto en la "legalidad aumentada"». *Actualidad Jurídica núm. 922*, Ed. Aranzadi, Cizur Menor, 2016.

DE PABLO CONTRERAS, P. (coord.), *Curso de Derecho Civil I Volumen II. Derecho de la Persona*, reimpresión de la 5ª edición., Ed. Edisofer, 2016.

DE VERDA Y BEAMONTE, J.R. (coord.), *Derecho al Honor: Tutela Constitucional, Responsabilidad Civil y Otras Cuestiones*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2015.

FERNÁNDEZ GARCÍA, A., «Sistemas de geolocalización como medio de control del trabajador: un análisis jurisprudencial», *Revista Aranzadi doctrinal social* núm. 17/2010, Ed. Aranzadi, Cizur Menor, 2010.

GARRIGA DOMÍNGUEZ, A. (coord.), *Fundamentos Éticos y Jurídicos de las TIC*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2012.

GRIMALT SERVERA, P., *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, 1ª edición, Ed. Iustel, 2007.

HERNÁNDEZ LÓPEZ, J.M., *El Derecho a la Protección de Datos Personales en la doctrina del Tribunal Constitucional*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2013.

HERRÁN ORTIZ, A.I., *El derecho a la intimidad en la nueva Ley Orgánica de Protección de datos personales*, Ed. Dykinson, Madrid, 2002.

LÓPEZ JIMÉNEZ, D., DITTMAR, E. C. "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital" en VALERO TORRIJOS, J. *La protección de los datos personales en internet ante la innovación tecnológica*, 1ª edición, Ed. Aranzadi, Cizur Menor, 2013.

MIERES MIERES, L.J., *Intimidad Personal y Familiar*, prontuario de Jurisprudencia Constitucional, Ed. Aranzadi, 2002.

REYES LÓPEZ, J.I. «Los dispositivos técnicos de geolocalización. Régimen Jurídico a partir de la L.O. 13/2015». *Revista Aranzadi Doctrinal* núm. 4, Ed. Aranzadi, Cizur Menor, 2016.