Papeles el tiempo de los derechos

PRIVACIDAD Y GEOLOCALIZACIÓN: ¿UN BINOMIO INCOMPATIBLE? ANÁLISIS DESDE LA FUNDAMENTALIDAD DE LOS DERECHOS AFECTADOS

María Concepción Torres Díaz
Profesora de Derecho Constitucional
Dpto. Estudios Jurídicos del Estado
Universidad de Alicante
concepcion.torres@ua.es

Palabras clave: Privacidad, Internet, Geolocalización, Derechos Humanos

Número: 6 Año: 2018

ISSN: 1989-8797

Comité Evaluador de los Working Papers “El Tiempo de los Derechos”

María José Añón (Universidad de Valencia)
María del Carmen Barranco (Universidad Carlos III)
María José Bernuz (Universidad de Zaragoza)
Manuel Calvo García (Universidad de Zaragoza)
Rafael de Asís (Universidad Carlos III)
Eusebio Fernández (Universidad Carlos III)
Andrés García Inda (Universidad de Zaragoza)
Cristina García Pascual (Universidad de Valencia)
Isabel Garrido (Universidad de Alcalá)
María José González Ordovás (Universidad de Zaragoza)
Jesús Ignacio Martínez García (Universidad of Cantabria)
Antonio E Pérez Luño (Universidad de Sevilla)
Miguel Revenga (Universidad de Cádiz)
Maria Eugenia Rodríguez Palop (Universidad Carlos III)
Eduardo Ruiz Vieytez (Universidad de Deusto)
Jaume Saura (Instituto de Derechos Humanos de Cataluña)

Privacidad y geolocalización: ¿un binomio incompatible? Análisis desde la fundamentalidad de los derechos afectados

María Concepción Torres Díaz
Profesora de Derecho Constitucional
Dpto. Estudios Jurídicos del Estado
Universidad de Alicante
concepcion.torres@ua.es

SUMARIO: I.- Planteamiento general. II.- Conceptualizaciones. III.- Contexto normativo: 3.1. La Directiva 95/46/CE y el Reglamento (UE) 2016/679 ante los datos de localización (y/o geolocalización). 3.2 La Directiva 2002/58/CE y los datos de localización (y/o geolocalización). IV.- Apuntos sobre el Dictamen 13/2011, de 16 de mayo, sobre los servicios de geolocalización en los dispositivos móviles inteligentes. V.- Consideraciones finales. VI.- Bibliografía.

I. PLANTEAMIENTO GENERAL

La Memoria Anual[1] de la Agencia Española de Protección de Datos correspondiente a 2011 recoge un apartado 3 en donde con el siguiente rótulo "Retos para la privacidad: las grandes cuestiones" aborda temas como el derecho al olvido, el cloud computing, los avances en el reconocimiento facial, los flujos internacionales de datos y los riesgos de la geolocalización. Pues bien, el presente artículo tiene como finalidad profundizar en esta última cuestión, esto es, poner de manifiesto los riesgos para la privacidad de la geolocalización de los dispositivos móviles inteligentes – tipo smartphones – y analizar el marco jurídico aplicable. Y es que el aumento de estos dispositivos – a nivel usuario/a – ha sido considerable en los últimos años, circunstancia que no ha pasado desapercibida para determinadas instituciones y organismos (AEPD, GT 29, etc.) que no han dudado en abordar esta cuestión en distintos informes, recomendaciones y dictámenes. En este sentido, conviene significar que estamos hablando de dispositivos

1 Véase la Memoria Anual de la Agencia Española de Protección de Datos correspondiente a 2011. Puede consultarse en la siguiente dirección electrónica: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf (fecha de consulta 30/04/2012).

inteligentes a través de los cuales se permite el acceso a múltiples servicios como conocer la previsión del tiempo, localizar amistades, encontrar direcciones, etc. La Memoria de la Agencia Española de Protección de Datos hace énfasis en que "la tecnología utilizada en estos terminales móviles, que están vinculados estrechamente a las personas, permite a los proveedores de servicios de geolocalización disponer de detalles de hábitos y pautas de comportamiento del propietario (…) y establecer perfiles exhaustivos (…)". Y es que la tecnología utilizada no es anodina sino que permite "(...) un control constante de los datos de localización mediante la captación de señales de estaciones de base y de puntos de acceso Wi-Fi". A tenor de lo expuesto surgen una serie de cuestiones que se erigen en puntos de reflexión en el presente artículo: ¿Cuál es el marco jurídico aplicable a los proveedores de servicios de geolocalización? ¿Qué tipo de datos – susceptibles de afectar a la privacidad de sus usuarios/as – almacenan? ¿Cuáles son los riesgos reales de una utilización sin control de este tipo de datos? ¿Se observa el "principio de privacidad desde el diseño" en el desarrollo de los dispositivos móviles inteligentes y en sus aplicaciones? ¿Existe conciencia – información y consentimiento previo – por parte de los usuarios/as ante la generación y almacenamiento de este tipo de datos? Sin duda, las cuestiones planteadas no son baladíes desde el punto de vista de la conceptualización del derecho a la protección de datos como derecho fundamental y desde la propia definición – en seno constitucional – de la privacidad. Máxime cuando se observa una cierta evolución en la propia normativa en materia de protección de datos que queda ejemplificada en la definición de dato de carácter personal que recoge la Directiva 95/46/CE[2] y que concreta – ampliando e introduciendo los llamados datos de localización (y/o geolocalización) – 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 y por el que se deroga la Directiva 95/46/CE[3].

2 Véase el artículo 2.a) de la Directiva 95/46/CE en donde se recoge el concepto de 'dato personal'. Señala que se entiende por tal *"toda información sobre una persona física identificada o identificable (el <<interesado>>); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social"*.

3 Sobre el Reglamento véase SEMPERE, F.J., *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la UE,* libro electrónico en Privacidad Lógica, 2013. Puede consultarse en la siguiente dirección url: http://www.privacidadlogica.es/2013/09/12/comentarios-practicos-a-la-propuesta-de-reglamento-de-proteccion-de-datos-de-la-ue-libro-descarga-gratuita/

II. CONCEPTUALIZACIONES

El título del presente trabajo delimita con bastante exactitud el contenido del mismo. Y es que bajo el rótulo "Privacidad y datos de geolocalización ¿un binomio incompatible? Análisis desde la fundamentalidad de los derechos afectados" se abordan una serie de cuestiones de especial importancia que obligan – en última instancia – a reflexionar sobre los riesgos para la privacidad de los datos de localización (y/o geolocalización). Al mismo tiempo, estas reflexiones requieren partir de una delimitación conceptual inserta en la sistemática constitucional de análisis. Un ámbito desde el que se perfila la tutela de los derechos fundamentales a través – entre otros – de un régimen de garantías[4] normativas, institucionales y jurisdiccionales previsto en el propio texto constitucional (artículos 53 y 54 CE). Un ámbito no exento de críticas pero, que en cualquier caso, necesita reconceptualizarse si se quiere tutelar con las máximas garantías los llamados datos de localización (y/o geolocalización).

Sin perjuicio de lo anterior, desde este ámbito conceptual resulta esencial delimitar una serie de términos. Entre ellos, cabría significar el concepto de privacidad, intimidad, datos de carácter personal y, muy especialmente, el concepto de datos de localización (y/o geolocalización). Estrechamente vinculados a los conceptos anteriores surgen con fuerza otros como el de consentimiento informado e información previa, principio de privacidad desde el diseño, neutralidad tecnológica y acceso universal a Internet.

Con respecto al concepto de privacidad cabe acudir – en primer lugar – al DRAE[5] quien lo define en los siguientes términos: "(...) ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Esta definición ofrece una primera aproximación con respecto al término estudiado. Término que nos invita a pensar en una estrecha conexión entre privacidad e intimidad. No obstante, sí cabe señalar cómo el término privacidad es bastante más amplio que el de intimidad. Y es que siguiendo a Y. NAVALPOTRO[6] la privacidad "(...) constituye un conjunto más

4 PÉREZ LUÑO, A.E., *Los derechos fundamentales,* Tecnos, Madrid, 2011.

5 Véase la definición de privacidad del DRAE, puede consultarse <http://buscon.rae.es/draeI/> [fecha de consulta 20/03/2011].

6 Véase NAVALPOTRO, Y., "Antecedentes de la Ley Orgánica 15/1999 (LOPD)", en ALMUZARA ALMAIDA, C., *Estudio práctico sobre la protección de datos de carácter personal,* Lex Nova, Madrid, 2005, p. 40.

amplio, más global, de facetas [de la personalidad de un individuo] que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado". Como señalaron S.D. WARREN y L.D. BRANDEIS[7] aludir a la 'privacy' es hacer referencia al derecho a ser dejado sólo (the right to be alone). Un derecho cuya recepción – desde el ámbito jurídico/constitucional – cabría extrapolar de la conjunción de varios derechos, a saber: intimidad, protección de datos, secreto de las comunicaciones y confidencialidad e integridad de los sistemas tecnológicos y de información. Y es que no se puede obviar la dimensión informacional que lleva implícita la privacidad. Una dimensión que permite vincular, en sede constitucional, privacidad con autotutela informativa o protección de datos así como con intimidad personal y familiar. Además, junto a esta dimensión informacional resulta esencial aludir a la dimensión espacial que la privacidad lleva de suyo. Dimensión que – incluso – adquiere una nueva significación cuando se tratan datos de localización (y/o geolocalización) por dos motivos fundamenalmente. Primero, porque incide en lo que se podría conceptuar como derecho al "anonimato situacional y/o espacial" y, segundo, porque afecta específicamente a dispositivos móviles por lo que la protección de éstos entran a formar parte de un nuevo ámbito espacial en donde ejercer la privacidad.

En lo que afecta al concepto de intimidad – en palabras del DRAE – es "(...) esa zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia". Esta definición ha sido precisada por el propio Tribunal Constitucional señalando que el derecho a la intimidad[8] reconoce el derecho a resguardar de la acción y

---

7 Véase WARREN, S.D. y BRANDEIS, L.D., "The Right to Privacy", *Harvard Law Review, 4,* 1890, pp. 193-220, citado en SERRANO PÉREZ, Mª M., *El derecho fundamental a la protección de datos. Derecho español y comparado*,Thompson-Civitas, 2003, pp. 29 y ss.

8 Véase el FJ 4 de la STC 115/2000 , de 5 de mayo., en donde recuerda el máximo intérprete constitucional como "(...) el derecho fundamental a la intimidad reconocido por el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona (art. 10.1 CE) frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar (SSTC 231/1988, de 2 de diciembre, y 197/1991, de 17 de octubre), frente a la divulgación del mismo por terceros y una publicidad no querida. No garantiza una intimidad determinada sino el derecho a poseerla, disponiendo a este fin un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 CE garantiza es, pues, el secreto sobre nuestra propia esfera de intimidad y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los lindes de nuestra vida privada". Véase también la STC 231/1988, de 2 de diciembre de 1988, en especial su FJ 4 cuando dispone textualmente: "(...) debe estimarse que, en principio, el derecho a la intimidad personal y familiar se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar, aspectos que, por la relación o vínculo existente con ellas, inciden en la

del conocimiento ajeno un ámbito propio y reservado de cada sujeto. Ámbito que se considera necesario para mantener una calidad mínima de vida humana según las pautas de nuestra conducta. Otro término a destacar es el concepto de datos de carácter personal[9]. Concepto que – desde el punto de vista de los derechos fundamentales – obliga a apelar a la autotutela informativa[10]. Derecho que atribuye a su titular un poder de disposición[11] y/o control de sus datos, esto es, a saber y ser informado sobre el destino y uso de los datos personales, el derecho de acceder, rectificar y cancelar los mismos, así como el derecho de oposición y a no verse sometido a una decisión con efectos jurídicos que se basen únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de la personalidad de los sujetos. Se observa, por tanto, como estamos – en el ámbito de la protección de datos – ante un derecho autónomo[12] y con sustantividad propia[13] que se inserta en ese ámbito más extenso – comentado en líneas anteriores – de 'privacidad'. Junto a los términos analizados cabe prestar especial

---

propia esfera de la personalidad del individuo que los derechos del art. 18 de la CE protege. Sin duda, será necesario, en cada caso, examinar de qué acontecimientos se trata, y cuál es el vínculo que une a las personas en cuestión, pero al menos, no cabe dudar que ciertos eventos que puedan ocurrir a padres, cónyuges o hijos tienen, normalmente, y dentro de las pautas culturales de nuestra sociedad, tal trascendencia para el individuo, que su indebida publicidad o difusión incide directamente en la propia esfera de su personalidad. Por lo que existe al respecto un derecho – propio, y no ajeno – a la intimidad, constitucionalmente protegible".

9 Sobre el concepto de dato de carácter personal véase el Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales. Puede consultarse en la siguiente dirección url: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf (Fecha de consutla 21/04/2013).

10 MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa,* Thomson/Civitas, Madrid, 2004.

11 Sobre el poder de disposición y control sobre los propios datos resulta de interés la STC 254/1993, de 20 de julio. Véase el FJ 7 en donde señala cómo "(...) El uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos". Continúa señalando cómo "(...) la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)".

12 Sobre el reconocimiento de fundamentalidad en el derecho a la protección de datos de carácter personal véase la STC 292/2000. El FJ 7 dispone textualmente "(...) el contenido del derecho a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Continúa señalando la sentencia referenciada en su FJ 7 que "(...) son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de los datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a oponerse a esa posesión y uso requerido a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de que datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o cancele".

13 SERRANO PÉREZ, M.M., *El derecho fundamental a la protección de datos. Derecho español y comparado,* Thomson-Civitas, Madrid, 2003.

atención a la expresión datos de localización (y/o geolocalización). Y es que bajo dicha terminología se alude a los datos que determinan el posicionamiento y/o la localización de un objeto espacial en un sistema de coordenadas determinado. En el ámbito jurídico la delimitación conceptual de datos de localización se recoge por primera vez en el artículo 2.c) de la Directiva 2002/58/CE[14], del Parlamento Europeo y del Consejo, de 12 de julio, 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)[15]. La dicción literal del precepto referenciado define el concepto de datos de geolocalización, disponiendo a tal efecto:

> "(...) cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario [a] de un servicio de comunicaciones electrónicas disponible para el público".

En el mismo sentido se pronuncia el artículo 64.b) del Real Decreto 424/2005[16], 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 usuarios/as. Define los 'datos de localización' en los siguientes términos "(...) cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario [a] de un servicio de comunicaciones electrónicas disponibles para el público".

Sin perjuicio de profundizar y analizar – en apartados posteriores – el concepto de datos de geolocalización, lo cierto y verdad es que la realidad más inmediata requiere la precisión de otros conceptos. De esta forma, cabe hacer referencia al consentimiento informado, principio de privacidad desde el diseño, neutralidad tecnológica y acceso universal a Internet. Con respecto a la delimitación conceptual de consentimiento informado cabe recurrir a la dicción literal del artículo 3.h) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal. En dicho precepto se

---

14 Puede consultarse la Directiva 2002/58/CE en la siguiente dirección electrónica: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:es:PDF (Fecha de consulta 22/07/2013).

15 Véase también la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores. Puede consultarse en la siguiente dirección url: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:Es:PDF (Fecha de consulta: 22/06/2013).

16 Puede consultarse el Real Decreto 424/2005 en la siguiente dirección url: http://www.boe.es/buscar/doc.php?id=BOE-A-2005-6970 (Fecha de consulta 20/06/2013).

define el consentimiento del interesado/a en los siguientes términos: "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado [a] consienta el tratamiento de datos personales que le conciernen". En el mismo sentido se pronuncia el artículo 6 en donde el consentimiento del interesado/a se erige en uno de los principios a tener en cuenta en materia de protección de datos. El párrafo 1 de dicho precepto dispone: "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado [a], salvo que la ley disponga otra cosa".

En lo que atañe al principio de privacidad desde el diseño[17], cabe precisar que mediante el mismo se trata de integrar – a nivel práctico – la protección de datos y la privacidad desde el comienzo mismo de las nuevas tecnologías de la información y comunicación[18]. En este sentido se pronuncia el Dictamen del Superior Europeo[19] de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad. Por tanto, conviene significar cómo para imponer el cumplimiento de este principio, se hace necesario adaptar el marco jurídico de protección de datos en aras de que efectivamente se integre el principio de privacidad desde el diseño con carácter vinculante e incorporándolo a determinados ámbitos de las TIC que presentan riesgos concretos y

17 Relacionado con la exigencia normativa de la privacidad desde el diseño cabe destacar el Dictamen 02/2013, sobre las aplicaciones de los dispositivos inteligentes. Puede consultarse en la siguiente dirección electrónica: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf (fecha de consulta 30/05/2013). Como recoge la Agencia Española de Protección de Datos en la nota sobre el Dictamen 02/2013 en dicho texto se analiza la incidencia y los riesgos que plantean para la protección de datos. El dictamen recoge "las obligaciones específicas tanto de los desarrolladores de aplicaciones como del resto de actores que intervienen en el desarrollo y la distribución de las mismas" entre los que cabe citar los creadores de apps, las tiendas de aplicaciones, los fabricantes de sistemas operativos y dispositivos y los proveedores de servicios publicitarios.

18 Véase TORRES DÍAZ, M.C., "El principio de privacidad desde el diseño en el marco del derecho a la protección de la confidencialidad e integridad de los sistemas tecnológicos y de información. ¿Ante un nuevo derecho fundamental?", en *Revista de Divulgación Informática,* Universidad de Alicante, 2010. Puede consultarse en la siguiente dirección url: http://revista.iuii.ua.es/es/articulos/2010/11/11/el-principio-de-privacidad-desde-el-disenyo-en-el-marco-del-derecho-a-la-proteccion-de-la-confidencialidad-e-integridad-de-los-sistemas-tecnologicos-y-de-informacion-Ante-un-nuevo-derecho-fundamental.html (fecha de consulta: 30/04/2012).

19 Véase el Dictamen del Supervisor Europeo de Protección de Datos, acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad (2010/C 280/01). Puede consultarse en la siguiente dirección electrónica: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:ES:PDF (fecha de consulta 02/03/2013). Véase también las recomendaciones del GT 29 sobre la necesidad de que el principio de privacidad desde el diseño sea vinculante para todos los diseñadores y diseñadoras así como productores y productoras de tecnología y sus responsables. Pueden consultarse las recomendaciones en el Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_es.pdf (fecha de consulta 22/04/2012).

que se atenuarían si se contara con una arquitectura técnica y un diseño adecuado. El Dictamen del Supervisor Europeo presta, en este sentido, una especial atención a la identificación por radiofrecuencia (RFID), a las aplicaciones de redes sociales y a las aplicaciones de navegación.

Con respecto a los conceptos de neutralidad tecnológica y acceso universal a las Internet cabe significar su estrecha relación conceptual. El DRAE remite al concepto 'neutral' cuando se realiza una búsqueda con la entrada 'neutralidad'. En su primera acepción lo define como "Que no participa de ninguna de las opciones en conflicto". Como señala C. CULLEL MARCH[20] la primera vez que se utilizó el concepto de neutralidad tecnológica fue en 1999 en un documento oficial de la Comisión Europea sobre la revisión del marco normativo de las comunicaciones electrónicas. Recuerda que este principio se adoptó "como uno de los cinco principios que regían el marco regulador de las comunicaciones electrónicas en la UE". Siguiendo el contenido de este primer texto, cabría perfilar un concepto de neutralidad tecnológica entendiendo por tal la no imposición y no discriminación en el uso de cualquier tipo de tecnología que permita el acceso y utilización de Internet, así como de aplicaciones, programas y servicios. Tanto la Directiva Marco 21/2002/CE como la Directiva 2009/140/CE lo incorporan como principio básico de regulación de las comunicaciones electrónicas. En nuestro ámbito jurídico interno cabe aludir al artículo 4.i) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en donde se dispone textualmente:

> "Principio de neutralidad tecnológica y de adaptabilidad al progreso de las técnicas y sistemas de comunicaciones electrónicas garantizando la independencia en la elección de las alternativas tecnológicas por los ciudadanos [as] y por las Administraciones Públicas, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos las Administraciones Públicas utilizarán estándares abiertos así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos".

20 CULLEL MARCH, C., "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico", en *Revista de Internet, Derecho y Política,* nº 11, 2010, Universitat Oberta de Catalunya.

Como señala E. GAMERO CASADO[21] "El principio tiene que ver (…) con los problemas de conectividad y compatibilidad" ya que las administraciones deben garantizar las relaciones con la ciudadanía y para ello es necesario que aseguren la compatibilidad de los equipos informáticos y la disponibilidad de software. Se observa, en este sentido, una estrecha conexión entre el principio de neutralidad tecnológica y el principio de igualdad y no discriminación. Y es que el fin último es evitar que el uso de medios electrónicos implique o suponga la existencia de restricciones o discriminaciones para la ciudadanía que opta por relacionarse con la Administración a través de medios electrónicos (versus artículo 4.b) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos).

Por último, y en lo que atañe al derecho de acceso universal[22] a Internet cabe precisar su conceptualización como derecho fundamental. Conceptualización que deviene del propio contexto internacional, en concreto, de la Declaración Conjunta sobre Libertad de Expresión e Internet de 1 de junio de 2011 (ONU). En el documento referenciado se conceptualiza el derecho de acceso como un derecho humano, instándose a los Estados a promover el acceso universal a Internet para garantizar el disfrute efectivo de otros derechos como la libertad de expresión, el derecho a la educación, la atención a la salud y el trabajo, el derecho de reunión y asociación así como el derecho a elecciones libres. Desde nuestro ámbito jurídico interno, aludir al derecho de acceso a Internet como derecho fundamental implica realizar una delimitación de su objeto, contenido, límites y bien jurídico protegido. Al mismo tiempo implica tener presente esa doble dimensión objetiva y subjetiva de la que son tributarios los derechos fundamentales y a las que hizo referencia el Tribunal Constitucional en la sentencia 25/1981 cuando expresamente señaló cómo los derechos fundamentales,

> "(...) son derechos subjetivos, derechos de los individuos en cuanto garantizan un status jurídico o la libertad de un ámbito de existencia. Pero, al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como un marco de una convivencia

21 GAMERO CASADO, E., "Objeto, ámbito de aplicación y principios generales de la Ley de Administración Electrónica: su posición en el sistema de fuentes", en GAMERO CASADO, E. y VALERO TORRIJOS, J., *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Pamplona, 2008, pp. 57-115.

22 TORRES DÍAZ, M.C., "El derecho de acceso a Internet como derecho fundamental: análisis constitucional desde una perspectiva crítica", en CORREIDORA Y ALFONSO, L. y COTINO HUESO, L., *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales,* Cuadernos y debates, nº 225, Centro de Estudios Políticos y Constitucionales, Madrid, 2013, pp. 3-21.

humana justa y pacífica, plasmada históricamente en el Estado de derecho y, más tarde, en el Estado social de derecho o el Estado social y democrático de derecho, según la fórmula de nuestra Constitución (art. 1.1)".

III. CONTEXTO NORMATIVO

Realizadas las anteriores precisiones conceptuales y terminológicas, conviene volver a focalizar el presente estudio en los datos de localización (y/o geolocalización) y, en concreto, en la normativa de referencia y/o aplicable. Normativa que obliga a precisar qué derechos fundamentales resultan afectados en el tratamiento de datos de geolocalización. De esta forma y en la medida en que los derechos susceptibles de verse afectados puedan ser la intimidad y el secreto de las comunicaciones habrá que tener en cuenta la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas (Directiva 2002/58/CE y Directiva 2009/136/CE) así como la normativa interna específica sobre este particular. Igualmente y, en la medida en que el derecho afectado pueda ser la protección de datos y/o la autotutela informativa, la normativa de referencia será la Directiva 95/46/CE y, más en concreto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril relativo a la protección de las personas físicas que deroga la anterior así como la normativa interna específica y conexa sobre este particular. En cualquier caso, y con independencia de los derechos específicos susceptibles de verse afectados, lo cierto y verdad es que en líneas generales cabría hablar de riesgos importantes – en el tratamiento de los datos de geolocalización – con respecto a ese concepto más amplio de privacidad[23].

3.1 La Directiva 95/46/CE y el Reglamento (UE) 2016/679 ante los datos de localización (y/o geolocalización)

Partiendo de las anteriores consideraciones procede analizar el contexto normativo aplicable en materia de datos de localización (y/o geolocalización). En este sentido procede referenciar los preceptos más significativos de la (derogada) Directiva 95/46/CE haciendo referencias específicas al Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre

23 Sobre el concepto de privacidad véase TORRES DÍAZ, M.C., "Privacidad y tracking cookies. Una aproximación constitucional", en CERRILLO-I-MARTÍNEZ, A., PEQUERA, M., PEÑA-LÓPEZ, I. & VILASAU SOLANA, M. (coords.), *Neutralidad de la red y otros retos para el futuro de Internet*. Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 11-12 de julio de 2011. Barcelona: UOC-Huygens, pp. 407-421.

circulación de estos datos. No obstante, cabe aludir previamente al artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) y al artículo 16.B[24] del Tratado de Lisboa. Y es que no hay duda de que los datos de localización (y/o geolocalización) son datos de carácter personal en la medida en que hacen a una persona identificada o identificable y, en tal sentido, generan riesgos no sólo en el ámbito específico del derecho a la protección de datos sino también en el derecho a la intimidad personal y familiar y en el derecho al secreto de las comunicaciones. Por tanto, las referencias normativas realizadas con anterioridad no resultan baladíes.

Entrando en el análisis de la Directiva 95/46/CE cabe destacar el contenido textual de los 'considerandos' 25 y 26. El 'considerando' 25 alude a las obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos. Obligaciones que se concretan en observar la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en la que se pueda efectuar el tratamiento. Al mimo tiempo, hace referencia a los derechos de los que son tributarios las personas cuyos datos sean objeto de tratamiento. Derechos que se concretan en el derecho de información, el derecho de acceso, rectificación y, en su caso, oposición. Con respecto al 'considerando' 26 dispone textualmente:

> "Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que no sea posible identificar al interesado [a]; que los códigos de conducta con arreglo al artículo 27 puedan constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificarse al interesado [a]".

24 El artículo 16.B del Tratado de Lisboa dispone textualmente: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organimos de la unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El control de dichas normas estará sometido al control de autoridades independientes".

Extrapolando estas consideraciones al ámbito que nos ocupa no cabe duda en cuanto a la identificación de los datos de localización (y/o geolocalización) con la delimitación conceptual de datos de carácter personal, en la medida en que la tecnología de los dispositivos móviles inteligentes – a través de la captación permanente de las señales procedentes de las estaciones base y de puntos de acceso Wi-Fi – hacen a una persona identificada o identificable. Y es que permiten su seguimiento siempre y cuando los servicios de localización estén activados.

Siguiendo con el análisis de la Directiva 95/46/CE cabe aludir a la dicción literal del 'considerando' 28. Dice textualmente:

> "Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal respecto al interesado [a], que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos, que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos, que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados".

La lectura del anterior considerando nos permite apuntar algunas consideraciones críticas con respecto al tratamiento de datos de geolocalización en la medida en que la captación de este tipo de datos a través de los teléfonos inteligentes no siempre es conocida por parte de los usuarios/as por lo que cabría cuestionar si se observan los requisitos de pertinencia y legitimidad junto a otros anteriormente referenciados. Otro 'considerando' relevante a los objetos de este artículo es el 'considerando' 30. En él se hace referencia al consentimiento[25] del interesado/a que otorga licitud al tratamiento de datos personales. Por tanto, cabría plantearse si ese consentimiento se recaba (se solicita expresamente a sus titulares) en el caso objeto de análisis, esto es, en el caso de los datos de geolocalización a través de los dispositivos inteligentes móviles y, en tal sentido, cómo se recaba. Sin duda son cuestiones relevantes desde el punto de vista de la fundamentalidad del derecho a la protección de datos. Fundamentalidad que no cabe cuestionar a tenor de la propia doctrina constitucional y, obviamente, de la fundamentalidad de otros derechos conexos como

25 Con respecto al consentimiento cabe aludir al apartado 25 de la propuesta de Reglamento. En dicho apartado se apela a la necesidad del consentimiento de forma explícita por cualquier medio apropiado que permita la manifestación libre, específica e informada de la voluntad del interesado/a. Se trata de garantizar que la persona sea consciente de que está dando su consentimiento al tratamiento de datos personales de tal forma que el silencio o la inacción no deba interpretarse como consentimiento.

intimidad y secreto de las comunicaciones, siendo más discutible en el caso de la confidencialidad e integridad de los sistemas tecnológicos y de información.

Sin perjuicio del contenido de otros 'considerandos' resulta pertinente tener en cuenta el articulado de la Directiva 95/46/CE en conexión con el nuevo Reglamento Europeo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales. En este sentido, resulta de interés aludir al artículo 1 que regula el objeto del mismo, así como al artículo 4 que recoge una serie de definiciones entre las que cabe destacar: datos personales, tratamiento de datos, fichero de datos personales, responsable del tratamiento, encargado/a del tratamiento, tercero, destinatario/a y consentimiento del interesado/a. Con respecto al concepto de datos personales cabe apuntar que se advierte una modificación en cuanto a su delimitación conceptual del Reglamento en relación a la Directiva. Y es que se observa cómo la nueva definición recogida en el Reglamento incluye – de forma expresa – como datos de carácter personal los datos de localización. En este sentido resulta pertinente acudir al artículo 4 apartados 1). Y es que define datos personales como toda información relativa a un interesado/a definiéndolo en los siguientes términos:

"(...) se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificar en línea o uno o varios elementos propios de la identidad física, fisiológica, enética, psíquieca, económica, cultural o social de dicha persona persona".

Con respecto a la delimitación conceptual recogida en la Directiva anterior se observa un cambio importante en la delimitación conceptual de 'datos de carácter personal'. Delimitación que lleva de suyo la incorporación de los datos de localización (y/o geolocalización) y, en tal sentido, requiere de la observancia de los principios y obligaciones recogidos en el actual Reglamento por parte de los proveedores de servicios de geolocalización.

3.2 La Directiva 2002/58/CE y los datos de localización (y/o geolocalización)

Con respecto a la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, 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), cabe citar – en primer lugar – el 'considerando' 14.

En dicho considerando ya se explicita lo que cabe entender cómo datos de localización (y/o geolocalización). Dispone su dicción literal:

> "Los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario [a], a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada".

Sin duda, el elenco de datos de localización evidencia la importancia de garantizar los derechos anteriormente referenciados, a saber, intimidad personal y familiar, protección de datos, secretos de las comunicaciones, etc. Derechos susceptibles de verse afectados ante un tratamiento inadecuado y/o abusivo por parte, en este caso, de los proveedores de los servicios de geolocalización. De ahí, que en la presente Directiva también se haga referencia al consentimiento del interesado/a. Consentimiento cuya primera alusión se encuentra en el 'considerando' 17 y cuyo tenor literal es el siguiente:

> "A efectos de la presente Directiva, el consentimiento de un usuario [a] o abonado [a], independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la Directiva 95/46/CE. El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario [a], por ejemplo mediante la selección de una casilla de un sitio web en Internet".

Se observa, por tanto, una clara remisión a la Directiva comentada anteriormente en lo que afecta al requisito del consentimiento, prueba evidente de la importancia del mismo en aras de garantizar esa autotutela informativa. Otro 'considerando' a tener en cuenta es el considerando 35 en donde se alude a las redes móviles digitales que tratan datos de localización y que proporcionan la posición geográfica del equipo terminal del usuario/a móvil para hacer posible la transmisión de las comunicaciones. Como se indica – tales datos – son, a su vez, datos de tráfico por lo que tienen la capacidad de tratar datos sobre localización con bastante precisión, utilizándose a través de servicios de valor añadido como ocurre con los servicios que ofrecen información sobre el tráfico. La Directiva señala que el tratamiento de tales datos "sólo debe permitirse cuando los abonados [as] hayan dado su consentimiento", precisando – además – que se debe facilitar un procedimiento para impedir temporalmente el tratamiento de los datos de

localización. Con respecto al análisis del articulado de la Directiva 2002/58/CE cabe citar, en primer lugar, el artículo 2 que recoge una serie de definiciones entre la que se encuentra la de datos de localización. El precepto referenciado – en su apartado c) – lo define en los siguientes términos: "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario [a] de un servicio de comunicaciones electrónicas disponibles para el público". Conexa con esta definición en el mismo precepto se encuentra la definición de datos de tráfico[26] así como la definición de comunicación. En segundo lugar, cabe aludir al artículo 9. En dicho precepto se hace referencia a los datos de localización distintos de los datos de tráfico. El párrafo primero de dicho precepto dispone:

> "1. En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios [as] o abonados [as] de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos o previo consentimiento de los usuarios [as] o abonados [as], en la medida y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios [as] o abonados [as], antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Se deberá ofrecer a los usuarios [as] y abonados [as] la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfrico".

En el párrafo 2 se recogen algunas consideraciones con respecto al consentimiento, indicándose la necesidad de establecer un procedimiento sencillo y gratuito en aras de rechazar temporalmente el tratamiento de los datos de localización.

Sin perjucio de lo expuesto, especial referencia cabe realizar del artículo 14 en donde se recogen una serie de consideraciones sobre características técnicas y normalización. En este sentido, cabe significar lo dispuesto en el párrafo 3 por cuanto recoge que se "(...) podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios [as] de proteger y

---

26 Véase el apartado b) del artículo 2. En dicho precepto se definen los datos de tráfico entendiendo por tal "cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma".

controlar el uso de sus datos personales de conformidad con la Directiva 1999/5/CE y la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones". Sin duda, cabría poner en relación este precepto con el principio de privacidad desde el diseño así como con el derecho a la confidencialidad e integridad de los sistemas tecnológicos y de información.

Con respecto al derecho a la confidencialidad e integridad de los sistemas tecnológicos y de información resulta de interés la Sentencia del Tribunal Constitucional alemán de 27 de febrero de 2008, que trae causa del recurso interpuesto contra la reforma de la Ley de los Servicios de Inteligencia del Estado de Renania del Norte de Westfalia, en virtud de la cual se autorizaba expresamente a tales servicios a que pudiesen utilizar de forma secreta spywares o troyanos para espiar los ordenadores sin que las personas afectadas fueran conscientes de ello con el fin de captar todo tipo de información susceptible de ser analizada en un momento posterior. El Tribunal declaró inconstitucional la reforma y se podría decir que configuró – de este modo – un nuevo derecho. Y es que al hilo de la dicción argumental del Tribunal de Karlsruhe[27] se observa que se da un paso más en el reconocimiento del derecho a la autodeterminación informativa cuyo ámbito de actuación se amplía a partir de esta sentencia a la protección absoluta de una zona nuclear del comportamiento privado que – en este caso – se extiende a los dispositivos informáticos terminales. De esta forma, se apela al derecho a la confidencialidad e integridad de los sistemas tecnológicos y de información, circunstancia que permite establecer una estrecha conexión de este derecho con el acceso a los datos de localización (y/o geolocalización) a través de dispositivos móviles.

IV. APUNTES SOBRE EL DICTAMEN 13/2011, DE 16 DE MAYO, SOBRE LOS SERVICIOS DE GEOLOCALIZACIÓN EN LOS DISPOSITIVOS MÓVILES INTELIGENTES

Realizadas las anteriores consideraciones con respecto a los datos de localización (y/o geolocalización) así como en lo que atañe a los derechos susceptibles de verse afectados, resulta pertinente – en estos momentos – analizar el Dictamen 13/2011 elaborado por el GP 29 sobre los servicios de geolocalización en los

27 PIÑAR MAÑAS, JL., *Seguridad, transparencia y protección de datos: el futuro de un escenario e incierto equilibrio*, en Documentos de trabajo 147/2009, Fundación Alternativas, Madrid, 2009.

dispositivos móviles inteligentes. En dicho dictamen se alude a los riesgos para la intimidad de las distintas infraestructuras de los datos procedentes de las tecnologías GPS y Wi-Fi a través de las cuales los usuarios/as acceden a los datos de geolocalización. Se observa como el concepto de intimidad[28] que maneja el dictamen es un concepto que cabría catalogar de "amplio" en conexión con el concepto de privacidad. Y es que se afirma la estrecha vinculación existente entre dispositivos móviles inteligentes y personas en la medida en que – actualmente – la mayoría de las personas disponen de dispositivos de estas características. Dispositivos en los que se suele almacenar una gran cantidad de información como documentos, fotografías, correos electrónicos, historial de navegación, etc. que revelan pautas de comportamiento y datos a través de los cuales se puede perfilar un retrato 'robot' de la personalidad de los sujetos afectados. Obviamente, esto determina que los proveedores de servicios de geolocalización puedan elaborar perfiles muy exhaustivos de la personalidad de los usuarios/as lo que cabe traducir – desde el punto de vista jurídico/constitucional y/o de tutela de los derechos fundamentales – en la necesidad de cumplir y observar una serie de exigencias introducidas en la normativa aplicable en aras de evitar cualquier tipo de vulneración de los derechos afectados.

Expuesto lo anterior conviene precisar que – en líneas generales – el marco jurídico aplicable es la Directiva sobre protección de datos (95/46/CE). Directiva aplicable en todos los supuestos de tratamiento de datos como consecuencia del tratamiento de datos de localización. Junto a esta Directiva cabe citar la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas (2002/58/CE) que será aplicable únicamente cuando afecte al tratamiento de datos de las estaciones de base por servicios y redes públicas de comunicaciones electrónicas, esto es, operadores de telecomunicaciones.

---

28 Sobre el derecho a la intimidad véase la STC de 7 de noviembre de 2011 en donde el máximo intérprete constitucional analiza si el ordenador personal constituye un medio idóneo de ejercicio de la intimidad personal. Señala en su FJ 3 que "(...) la intimidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado". El TC matiza cómo el avance de la tecnología actual ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad. De ahí que el TC haga hincapié en que "(...) el reconocimiento global de un derecho a la intimidad o a la vida privada [debe abarcar] las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida". Sobre esta sentencia véase TORRES DÍAZ, MC., "Análisis constitucional de la intimidad personal a propósito de la Sentencia del Tribunal Constitucional de 7 de noviembre de 2011", en TERUEL LOZANO, GM., PÉREZ MIRAS, A. y CARLO RAFFIOTA, E., *Desafíos para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías,* Thomson-Reuters, Aranzadi, Pamplona, 2013, pp. 127-137.

Con respecto a las obligaciones que se derivan de la legislación sobre protección de datos cabe diferenciar – como recoge el Dictamen 13/2011 – las obligaciones del responsable del tratamiento de datos de las infraestructuras de geolocalización, las obligaciones del proveedor de una aplicación o un servicio específico de geolocalización así como las obligaciones que se derivan para los creadores de un sistema operativo de un dispositivo móvil inteligente. En lo que atañe a las obligaciones del responsable de un tratamiento de datos de las infraestructuras de geolocalización habrá que estar a lo dispuesto en el artículo 2.d) de la Directiva sobre protección de datos. Y es que no cabe olvidar que los responsables de tratamientos de datos de las infraestructuras de geolocalización en el momento en que procesan la localización de los dispositivos móviles a través de estaciones base, GPS o a través de puntos de acceso Wi-Fi procesan datos personales. Por su parte, los proveedores de aplicaciones y servicios de geolocalización que facilitan la instalación de programas informáticos a terceros también procesan datos de localización de los dispositivos móviles inteligentes como puede ser el caso de los servicios de previsiones metereológicas. A tenor de la normativa vigente, el proveedor de una aplicación que sea capaz de procesar datos de geolocalización será responsable del tratamiento de los datos de geolocalización que resulten de su instalación y uso. Por último, en cuanto a los creadores de sistemas operativos de dispositivos móviles inteligentes serán responsables del tratamiento de datos de geolocalización cuando interactúen directamente con el usuario/a y recojan datos personales. En este sentido, deberá observarse el principio de privacidad desde el diseño en aras de evitar controles secretos por parte del propio dispositivo o, en su caso, por parte de las aplicaciones y/o servicios como puede ser la adaptación y/o actualización horaria automática en función de la localización.

El Dictamen 13/2011 del GT 29 amplía la serie de responsables en la medida en que también tratan datos de geolocalización. Entre estos responsables se encuentran determinadas plataformas[29] como navegadores, redes sociales[30] así como los medios de comunicación que permitan el etiquetado geográfico[31]. El Dictamen señala

29 Sobre privacidad y redes sociales véase RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. (coords.), *Derecho y Redes Sociales,* Thomson Reuters-Civitas, Madrid, 2010.

30 Con respecto a los datos de geolocalización que se tratan a través de las redes sociales resulta interesante la acuñación de las acepciones 'geolocalización social' y/o 'geosocialización'. Relacionado con las anteriores acepciones cabe significar también el denominado geocommerce, esto es, la venta de productos y servicios en función de la localización de las y los clientes.

31 Sobre la geolocalización a través del etiquetado geográfico (geo etiquetar o geo taggear) resulta interesante tener en cuenta los dispositivos móviles que disponen de cámaras con GPS ya que – en estos

expresamente que cuando estas plataformas incorporan mecanismos de geolocalización "tienen la importante responsabilidad de decidir sobre los parámetros de la aplicación (activación o desactivación por defecto)".

A tenor de todo lo comentado conviene precisar que los operadores de telecomunicaciones que quieran utilizar datos de estaciones bases para prestar un servicio de valor añadido a través de los dispositivos móviles deberán obtener el consentimiento previo de los usuarios/as. Al mismo tiempo, deberán cerciorarse de que los usuarios/as cuentan con la información requerida en la normativa referenciada. Y es que no se puede olvidar que el tratamiento de datos de localización (y/o geolocalización) afecta a una serie de derechos entre los que se encuentran (básicamente) el derecho a la autotutela informativa (protección de datos) y el derecho a la intimidad personal y familiar. Derechos que gozan de fundamentalidad en nuestro texto constitucional ya que así se deriva del articulado constitucional y de la propia doctrina y jurisprudencia de referencia. En este sentido, no resulta extraño que el consentimiento se erija, por un lado, en un límite al tratamiento de los datos de geolocalización y, por otro, en una obligación para los prestadores de servicios de geolocalización. Ahora bien ¿qué requisitos deberán observarse con respecto a la prestación del consentimiento? La respuesta no resulta baladí a tenor de lo que disponía la dicción literal del artículo 2.h) de la Directiva 95/46/CE en donde se conceptualizaba el consentimiento como una "manifestación de voluntad, libre, específica e informada, mediante la que el interesado [a] consienta el tratamiento de datos personales que le conciernan" y más en concreto con respecto al contenido del actual Reglamento que añade algunos elementos importantes a tener en cuenta cuando delimita el consentimiento del interesado [a] en los siguientes términos: "(...) toda manifestación libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". En esta misma línea cabe aludir a las condiciones recogidas en el artículo 7 del Reglamento relativas a la valoración de la prestación del consentimiento[32]. No obstante, el problema surgirá cuando el dispositivo móvil sea capaz de transformar y transmitir datos de localización procedentes de terceros sin que

casos – el etiquetado al realizar fotografías es automático y, en muchas ocasiones, los usuarios/as desconocen el mismo con los riesgos que conlleva para su privacidad.

32 Sobre este particular téngase en cuenta la obligación del responsable del tratamiento de demostrar que el interesado consintió el tratamiento de sus datos personales, en este caso, datos de geolocalización.

el interesado/a haya manifestado expresamente su consentimiento libre e informado. Se advierte – en estos casos – la necesidad de observar el principio de privacidad desde el diseño tanto en los dispositivos móviles, como en las aplicaciones y/o servicios que permitan tratar y/o procesar datos de localización así como el derecho a la integridad y confidencialidad de los sistemas tecnológicos y de información.

Aludía – en líneas anteriores – a cómo el consentimiento se erige en una garantía para los titulares de los datos de localización y en una obligación para los prestadores de servicios de localización. Pues bien, en la misma línea cabe hablar sobre el requisito de la información previa. Información que se concreta en una garantía de los derechos susceptibles de verse afectados y – al mismo tiempo – en una obligación que va destinada a informar sobre los fines del tratamiento y sus destinatarios/as. Información que deberá ser legible y que deberá permitir acceder a los perfiles sobre la base de los datos de localización en aras de que el usuario/a pueda actualizar, rectificar o suprimir dicha información.

Otro aspecto importante que se aborda en el Dictamen es el relativo a los períodos de retención[33] de los datos de localización. El dictamen señala que "los proveedores de servicios de geolocalización y de aplicaciones deben determinar el período de retención de datos de localización" puntualizando que éste no deberá ser superior al necesario para los fines para los que fueron recogidos o para los que se puedan tratar posteriormente. En este sentido, se insta a que los datos de localización y de perfiles obtenidos sean suprimidos después de un período justificado. Esta supresión resulta especialmente relevante cuando los datos de localización se obtienen a través del la asociación de una dirección MAC con distintos puntos de acceso WiFi puesto que la no supresión de una localización anterior puede derivar en un uso abusivo de este tipo de datos dirigidas, por ejemplo, a actividades de mercadotecnia como se señala en el Dictamen 13/2011 del GT 29.

33 Sobre la retención de datos consúltese la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de mayo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE. En nuestro ámbito jurídico interno véase la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

V. CONSIDERACIONES FINALES

Al inicio del presente artículo planteaba las siguientes cuestiones: ¿Cuál es el marco jurídico aplicable a los proveedores de servicios de geolocalización? ¿Qué tipo de datos – susceptibles de afectar a la privacidad de sus usuarios/as – almacenan? ¿Cuáles son los riesgos reales de una utilización sin control de este tipo de datos? ¿Se observa el "principio de privacidad desde el diseño" en el desarrollo de los dispositivos móviles inteligentes y en sus aplicaciones? ¿Existe conciencia – información y consentimiento previo – por parte de los usuarios/as ante la generación y almacenamiento de este tipo de datos? Pues bien, llegados a este punto – y al hilo de lo comentado en párrafos anteriores – sí estaríamos en disposición de esbozar las respuestas – en sede constitucional – a las cuestiones planteadas. Respuestas que parten de la consideración de la fundamentalidad de los derechos afectados y que parten – al mismo tiempo – del reconocimiento de la afectación de los datos de localización (y/o geolocalización) a la privacidad de las personas en la medida en que estos dispositivos móviles están vinculados – en la mayoría de ocasiones – a una persona física. En este sentido cabe colegir:

- La normativa aplicable de referencia actual es el Reglamento (UE) 2016/679[34] de 27 de abril, 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 conexión con la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995. No obstante, también hay que observar la Directiva 2002/58/CE en los supuestos en los que el tratamiento de datos de localización se realiza a través de estaciones de bases por operadores de telecomunicaciones. Obviamente – y circunscribiendo el marco normativo aplicable a nuestro ámbito jurídico interno – habrá que tener en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal así como el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

34 Puede consultarse 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 y por el que se deroga la Directiva 95/46/CE en el siguiente enlace. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES (fecha de consulta: 22/09/2017).

- Con respecto al tipo de datos de localización que los proveedores de servicios de localización tratan, cabe destacar: datos geográficos de localización (país, Estado o provincia, ciudad, dirección, código postal, etc), datos sobre IP, datos sobre latitud y longitud, datos sobre cambio de posición, etc. Junto a esos datos cabe especificar otros que también son objeto de tratamiento como: nombre y apellidos, dirección postal, número de tarjeta de crédito, dirección MAC, teléfono, correo electrónico, etc. No cabe duda que – en la medida en que este tipo de datos identifiquen o permitan identificar a una persona (de forma directa o indirecta) – estaremos ante datos de carácter personal, circunstancia que permite aludir tanto al derecho a la autotutela informativa como al derecho a la intimidad personal y familiar, sin olvidar otros derechos conexos y susceptibles de verse afectados tales como secreto de las comunicaciones y la confidencialidad e integridad de los sistemas tecnológicos y de información.

- En lo que afecta a la observación del principio de privacidad desde el diseño cabe señalar que se perfila como una garantía específica y, por ende, como una exigencia en aras de la tutela de los derechos referenciados.

- En lo que atañe a los requisitos de consentimiento e información previa, cabe apuntar su doble consideración. Por un lado, como garantía de los derechos susceptibles de verse afectados y, por otro, como una obligación a observar por parte de los proveedores de este tipo de servicios.

- Con respecto a la fundamentalidad de los derechos afectados cabe destacar que – desde la sistemática constitucional de análisis – tanto el derecho a la intimidad como el derecho a la autotutela informativa son conceptualizados como derechos fundamentales. Por tanto, desde el punto de vista axiológico (fundamento objetivo) son exponentes de ese pacto social que legitima nuestro Estado social y democrático de Derecho. Lo mismo cabe apuntar con respecto al derecho al secreto de las comunicaciones. No obstante, apelar a la fundamentalidad del derecho a la integridad y confidencialidad de los sistemas tecnológicos y de información parece más discutido puesto que para un amplio sector doctrinal este derecho se insertaría en el derecho a la intimidad. En cualquier caso, desde la perspectiva subjetiva cabe precisar cómo los diferentes derechos susceptibles de verse afectados por el tratamiento de los datos de localización son derechos

que atribuyen un determinado estatus jurídico a los sujetos afectados/as y, por ende, se erigen en garantías que permiten tutelar la libertad, la autonomía y seguridad de los mismos frente a cualquier uso abusivo de este tipo de datos, esto es, frente a cualquier abuso de poder ante el tratamiento de los datos de localización (y/o geolocalización).

- Por último, y relacionado con el punto anterior (fundamentalidad de los derechos afectados), cabe resaltar la dimensión informacional y espacial que lleva implícita la privacidad. Máxime si los riesgos relativos a la privacidad derivan del tratamiento de los datos de localización (y/o geolocalización). Con respecto a la dimensión espacial cabe prestar especial atención a dos aspectos. En primer lugar, a la incidencia en lo que se podría conceptuar como derecho al "anonimato situacional y/o espacial" y, en segundo lugar, al ámbito espacial electrónico/digital en donde ejercer y tutelar la privacidad.

VI. BIBLIOGRAFÍA

- CULLEL MARCH, C., "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico", en *Revista de Internet, Derecho y Política,* nº 11, 2010, Universitat Oberta de Catalunya.

- Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales. Puede consultarse en la siguiente dirección url: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf (Fecha de consutla 21/04/2013).

- Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp150_es.pdf (fecha de consulta 22/04/2012).

- Dictamen del Supervisor Europeo de Protección de Datos, acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad (2010/C 280/01). Puede consultarse en la siguiente dirección electrónica: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:280:0001:0015:ES:PDF (fecha de consulta 02/03/2013).

- Dictamen 02/2013, sobre las aplicaciones de los dispositivos inteligentes. Puede consultarse en la siguiente dirección electrónica: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_es.pdf (fecha de consulta 30/05/2013).

- GAMERO CASADO, E., "Objeto, ámbito de aplicación y principios generales de la Ley de Administración Electrónica: su posición en el sistema de fuentes", en GAMERO CASADO, E. y VALERO TORRIJOS, J., *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Pamplona, 2008, pp. 57-115.

- MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa,* Thomson/Civitas, Madrid, 2004.

- Memoria Anual de la Agencia Española de Protección de Datos correspondiente a 2011. Puede consultarse en la siguiente dirección electrónica: http://www.agpd.es/portalwebAGPD/canaldocumentacion/memorias/memoria_2011/common/Memoria_2011.pdf (fecha de consulta 30/04/2012).

- NAVALPOTRO, Y., "Antecedentes de la Ley Orgánica 15/1999 (LOPD)", en ALMUZARA ALMAIDA, C., *Estudio práctico sobre la protección de datos de carácter personal,* Lex Nova, Madrid, 2005.

- PÉREZ LUÑO, A.E., *Los derechos fundamentales,* Tecnos, Madrid, 2011.

- PIÑAR MAÑAS, J.L., *Seguridad, transparencia y protección de datos: el futuro de un escenario e incierto equilibrio*, en Documentos de trabajo 147/2009, Fundación Alternativas, Madrid, 2009.

- RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. (coords.), *Derecho y Redes Sociales,* Thomson Reuters/Civitas, Madrid, 2010.

- 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 en el siguiente enlace. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES (fecha de consulta: 22/09/2017).

- SEMPERE, F.J., *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la UE,* libro electrónico en Privacidad Lógica, 2013. Puede consultarse en la siguiente dirección url: http://www.privacidadlogica.es/2013/09/12/comentarios-practicos-a-la-propuesta-de-reglamento-de-proteccion-de-datos-de-la-ue-libro-descarga-gratuita/

- SERRANO PÉREZ, M.M., *El derecho fundamental a la protección de datos. Derecho español y comparado,* Thomson-Civitas, Madrid, 2003.

- TORRES DÍAZ, M.C., "El principio de privacidad desde el diseño en el marco del derecho a la protección de la confidencialidad e integridad de los sistemas tecnológicos y de información. ¿Ante un nuevo derecho fundamental?", en *Revista de Divulgación Informática,* Universidad de Alicante, 2010.

- TORRES DÍAZ, M.C., "Privacidad y tracking cookies. Una aproximación constitucional", en CERRILLO-I-MARTÍNEZ, A., PEGUERA, M., PEÑA-LÓPEZ, I. & VILASAU SOLANA, M. (coords.), *Neutralidad de la red y otros retos para el*

futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 11-12 de julio de 2011. Barcelona: UOC-Huygens, pp. 407-421.

- TORRES DÍAZ, M.C., "El derecho de acceso a Internet como derecho fundamental: análisis constitucional desde una perspectiva crítica", en CORREIDORA Y ALFONSO, L. y COTINO HUESO, L., *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales,* Cuadernos y debates, nº 225, Centro de Estudios Políticos y Constitucionales, Madrid, 2013, pp. 3-21.

- TORRES DÍAZ, MC., "Análisis constitucional de la intimidad personal a propósito de la Sentencia del Tribunal Constitucional de 7 de noviembre de 2011", en TERUEL LOZANO, GM., PÉREZ MIRAS, A. y CARLO RAFFIOTA, E., *Desafíos para los derechos de la persona ante el siglo XXI: Internet y nuevas tecnologías,* Thomson-Reuters, Aranzadi, Pamplona, 2013. pp. 127-137.

- WARREN, S.D. y BRANDEIS, L.D., "The Right to Privacy", *Harvard Law Review, 4,* 1890, pp. 193-220, citado en SERRANO PÉREZ, Mª M., *El derecho fundamental a la protección de datos. Derecho español y comparado*,Thompson-Civitas, 2003.