Grupo de trabajo sobre protección de datos establecido por el ARTÍCULO 29

**881/11/ES**
**WP 185**

# Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes

**Adoptado el 16 de mayo de 2011**

**CONTENTS**

**EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES,**
establecido por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995,

Vistos el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3 de dicha Directiva,

Visto su Reglamento interno,

**HA ADOPTADO EL PRESENTE DOCUMENTO:**

## 1. Introducción

La información geográfica juega un papel importante en nuestra sociedad. Casi todas las actividades y decisiones humanas tienen un componente geográfico. En general, el valor de la información aumenta cuando está ligada a una localización y toda localización puede ligarse a cualquier tipo de información: datos financieros, de salud o sobre el comportamiento de los consumidores. Con el rápido desarrollo tecnológico y la amplia difusión de dispositivos móviles inteligentes, se está desarrollando una nueva categoría de servicios basados en la localización.

El objetivo del presente dictamen es aclarar el marco jurídico aplicable a los servicios de geolocalización disponibles en dispositivos móviles inteligentes (o que son generados por éstos) que se pueden conectar a Internet y están equipados con sensores de localización tales como el GPS. Ejemplos de estos servicios son: mapas y navegación, servicios geográficos personalizados (como puntos de interés próximos), realidad aumentada, etiquetado geográfico de contenidos en Internet, rastreo del paradero de amigos, control de los hijos y publicidad basada en la ubicación.

El dictamen también se ocupa de los tres principales tipos de infraestructuras destinadas a prestar servicios de geolocalización: GPS, estaciones de base GSM y WiFi, poniendo una especial atención en la nueva infraestructura basada en la ubicación de puntos de acceso WiFi.

El Grupo de trabajo es plenamente consciente de que hay muchos otros servicios que procesan datos de localización que también pueden plantear problemas de protección de datos y que van desde los sistemas de billetería electrónica hasta los sistemas de peaje para automóviles, o desde servicios de navegación por satélite hasta el seguimiento de la posición, por ejemplo con ayuda de cámaras, y la geolocalización de direcciones IP. Sin embargo, habida cuenta de la rápida evolución tecnológica, en particular la cartografía de los puntos de acceso inalámbrico, en combinación con el hecho de que los nuevos operadores en el mercado se preparan para desarrollar nuevos servicios de localización que utilizan una combinación de datos procedentes de estaciones de base, GPS y WiFi, el Grupo de trabajo ha decidido aclarar específicamente los requisitos legales para dichos servicios en virtud de la Directiva sobre protección de datos.

El dictamen describe en primer lugar la tecnología, posteriormente identifica y evalúa los riesgos para la intimidad y luego expone las conclusiones sobre la aplicación de la legislación a los distintos responsables del tratamiento que recopilan y procesan datos sobre localización procedentes de dispositivos móviles. Esto incluye, por ejemplo, a los proveedores de infraestructuras de geolocalización, los fabricantes de teléfonos inteligentes y los creadores de aplicaciones de geolocalización.

El dictamen no evalúa la tecnología de etiquetado geográfico específico vinculada a la denominada Web 2.0, en la que los usuarios integran información con referencias geográficas en redes sociales como Facebook o Twitter. Tampoco entra en detalles sobre algunas otras tecnologías de geolocalización que se utilizan para interconectar productos en una superficie relativamente pequeña (centros comerciales, aeropuertos, edificios de oficinas, etc.), como Bluetooth, Zigbee, el «perimetraje», y las etiquetas inteligentes con tecnología WiFi, aunque muchas de las conclusiones del dictamen con respecto a las razones jurídicas, la información y los derechos de las personas también se aplican a estas tecnologías cuando se utilizan para la geolocalización de personas a través de sus dispositivos.

## 2. Contexto: diferentes infraestructuras de geolocalización

### 2.1 Datos procedentes de estaciones de base

El área cubierta por los diferentes operadores de telecomunicaciones está dividida en partes que se conocen generalmente como «casillas». Para poder utilizar un teléfono móvil o conectarse a Internet mediante un dispositivo de comunicación 3G, el dispositivo móvil ha de conectarse a la antena (en lo sucesivo denominada «estación de base») que cubre dicha casilla. Las casillas tienen distintos tamaños en función de las interferencias que se producen, por ejemplo, con montañas y edificios altos.

Durante todo el tiempo en que un dispositivo móvil permanece encendido, está en conexión permanente con una determinada estación de base y el operador de telecomunicaciones lleva un registro continuo de estas conexiones. Cada estación de base tiene un número de identificación único y está registrada con una ubicación específica. Tanto el operador de telecomunicaciones como muchos dispositivos móviles son capaces de utilizar las señales de casillas (estaciones de base) solapadas para estimar la posición del dispositivo móvil con mayor precisión. Esta técnica también se denomina «triangulación».

La precisión puede incrementarse con la ayuda de parámetros como la intensidad de señal recibida, la diferencia en el tiempo de llegada de la señal y el ángulo de entrada de la señal.

Los datos de la estación de base pueden utilizarse en formas innovadoras, por ejemplo para detectar atascos de tráfico, ya que cada carretera presenta una velocidad media para cada hora del día, pero cuando la conmutación a la siguiente estación de base lleva más tiempo del esperado suele estarse en presencia de un embotellamiento.

En suma, este método de posicionamiento da una idea rápida y general de la ubicación, pero no es muy preciso en comparación con los datos GPS y WiFi. La

precisión es de aproximadamente 50 metros en las zonas urbanas densamente pobladas y de hasta varios kilómetros en las zonas rurales.

## 2.2 Tecnología GPS

Los dispositivos móviles inteligentes disponen de una serie de microprocesadores con receptores de GPS que determinan su ubicación.

La tecnología GPS (sistema de posicionamiento global por satélite, GPS en sus siglas inglesas) utiliza 31 satélites que giran en 6 órbitas diferentes alrededor de la Tierra[1]; cada satélite transmite una señal radioeléctrica muy precisa.

El dispositivo móvil puede determinar su ubicación cuando la antena del GPS recibe al menos 4 de dichas señales. Esta señal es diferente de los datos de las estaciones de base porque solo viaja en un sentido. Las entidades que gestionan los satélites no tienen capacidad para establecer un registro de los dispositivos que han recibido la señal radioeléctrica.

La tecnología GPS ofrece un posicionamiento exacto, de entre 4 y 15 metros, y su principal desventaja es que su arranque es relativamente lento[2]. Otro inconveniente es que no funciona o funciona mal en lugares cerrados. Por ello, en la práctica la tecnología GPS se combina a menudo con datos de estaciones de base o puntos de acceso WiFi cartografiados.

## 2.3 WiFi

### 2.3.1 Puntos de acceso WiFi

Una fuente de información a efectos de geolocalización relativamente nueva es el uso de los puntos de acceso WiFi. La tecnología es similar al uso de estaciones de base. Ambas se valen de un número de identificación único (de la estación de base o del punto de acceso WiFi) que puede ser detectado por un dispositivo móvil y ser enviado a un servicio que conoce la ubicación de cada uno de estos puntos de identificación únicos.

La identificación única de cada punto de acceso WiFi es su dirección de control de acceso al medio («dirección MAC», por la siglas inglesas de *Medium Access Control*). La dirección MAC es un identificador único asignado a una interfaz de red y

[1] El sistema de posicionamiento global consiste en satélites lanzados por Estados Unidos, para fines militares. En 2014, la Comisión Europea tiene previsto lanzar Galileo, una red de 18 satélites que ofrecerá un sistema mundial de radionavegación por satélite gratuito y de uso civil. Los 2 primeros satélites se lanzarán en 2011 y otros 2 lo serán en 2012. Fuente: Comisión Europea, La Comisión presenta la revisión intermedia de los programas Galileo y EGNOS, 25 de enero de 2011, URL: http://ec.europa.eu/enterprise/newsroom/cf/itemlongdetail.cfm?displaytype = noticias y el AT_id = 0 & item_id = 4835

[2] Con el fin de acelerar la detección inicial de la señal GPS, es posible cargar previamente las llamadas «tablas arco iris», que contienen la posición esperada de los diferentes satélites en las semanas siguientes.

normalmente registrada en componentes como microprocesadores de memoria o tarjetas de red en ordenadores, teléfonos, ordenadores portátiles o puntos de acceso[3].

La razón por la que los puntos de acceso WiFi pueden ser utilizados como una fuente de información a efectos de geolocalización es porque anuncian continuamente su existencia. La mayoría de los puntos de acceso a Internet por banda ancha también incluyen de oficio una antena WiFi. Por defecto, los puntos de acceso más comúnmente utilizados en Europa tienen activada la conexión, incluso cuando el usuario solo ha conectado su ordenador mediante cables al punto de acceso. Al igual que una radio, un punto de acceso WiFi transmite continuamente su propio nombre de red y su dirección MAC, incluso cuando nadie esté utilizando la conexión o cuando el contenido de las comunicaciones inalámbricas esté cifrado mediante WEP, WPA o WPA2.

Hay dos formas distintas de recopilar las direcciones MAC de los puntos de acceso WiFi[4]:

1. Barrido activo: envío de solicitudes activas[5] a todos los puntos de acceso WiFi cercanos y registro de sus respuestas. Estas respuestas no incluyen información sobre los dispositivos conectados al punto de acceso WIFI.

2. Barrido pasivo: registro de las señales transmitidas periódicamente por cada punto de acceso (generalmente 10 veces por segundo). Como alternativa y excepcionalmente, algunos dispositivos registran todas las señales WiFi transmitidas por los puntos de acceso, incluidos los que no emitan señales de baliza. Si este tipo de barrido se realiza sin aplicar adecuadamente la protección de la intimidad desde el diseño, ello puede desembocar en la obtención de datos intercambiados entre los puntos de acceso y los aparatos conectados a ellos. De esta manera podrían registrarse las direcciones MAC de los ordenadores, ordenadores portátiles e impresoras. Este tipo de barrido también podría conducir al registro ilegal del contenido de las comunicaciones. Estos contenidos son fácilmente legibles en caso de que el propietario del punto de acceso WiFi no haya activado un cifrado WiFi (WEP/WPA/WPA2).

La ubicación de un punto de acceso WiFi puede calcularse de dos formas diferentes.

1. Estáticamente y una sola vez: los propios responsables del tratamiento de datos recopilan las direcciones MAC de los puntos de acceso WiFi desplazándose con vehículos equipados con antenas. Se registran la latitud y longitud exactas del vehículo el momento en que se recibe la señal y así se puede calcular la ubicación de los puntos de acceso utilizando, entre otros datos, la intensidad de la señal.

---

3 Un ejemplo de dirección MAC es: 00-1F-3F-D7-3C-58. La dirección MAC de un punto de acceso WiFi se denomina BSSID (identificador del dispositivo de servicios básicos).

4 El barrido activo y pasivo han sido normalizados mediante la norma IEEE 802.11 con objeto de detectar los puntos de acceso.

5 Con el fin de recopilar las direcciones MAC, el receptor envía una «solicitud sonda» a todos los puntos de acceso.

2. Dinámica y continuamente: los usuarios de servicios de geolocalización recogen automáticamente las direcciones MAC captadas por sus dispositivos WiFi cuando, por ejemplo, utilizan un mapa en línea para determinar su propia posición (¿Dónde estoy?). El dispositivo móvil envía toda la información disponible al proveedor del servicio de geolocalización, incluida la dirección MAC, las SSID y la intensidad de señal. El controlador puede usar estas consultas en curso para calcular o mejorar la localización de los puntos de acceso WiFi en su base de datos.

Es importante señalar que los dispositivos móviles no necesitan «conectarse» a puntos de acceso WiFi para recoger información WiFi ya que detectan automáticamente la presencia de dichos puntos (en modo de barrido activo o pasivo) y automáticamente recogen datos sobre ellos.

Además, los teléfonos móviles que solicitan ser geolocalizados no solo enviarán datos WiFi, sino también, a menudo, cualquier otra información sobre localización de la que dispongan, incluidos los datos sobre GPS y estaciones de base. Ello permite al prestador calcular la localización de «nuevos» puntos de acceso WiFi o mejorar la localización de los puntos que ya estaban incluidos en la base de datos. De este modo, la recogida de información sobre puntos de acceso WiFi está descentralizada de una forma muy eficiente, sin que los consumidores tengan conocimiento de ello necesariamente.

En resumen: la geolocalización mediante el uso de puntos de acceso WiFi ofrece una localización rápida y cada vez más precisa basada en mediciones continuas.

## 3. Riesgos para la intimidad

Los dispositivos móviles inteligentes están muy estrechamente vinculados a las personas porque la mayoría de ellas tienden a mantener su dispositivo móvil muy cerca de ellas, en el bolsillo, en el bolso o sobre la mesilla de noche.

Raramente ocurre que una persona preste su dispositivo a otra. La mayoría de las personas son conscientes de que su dispositivo móvil contiene una gran cantidad de información, desde mensajes electrónicos hasta fotografías privadas, o desde un historial de navegación por Internet hasta, por ejemplo, una lista de contactos.

Esto permite a los proveedores de servicios de geolocalización disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un período de inactividad nocturna puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir asimismo datos derivados de las pautas de movimientos de sus amigos, sobre la base de lo que se conoce como «gráfica social»[6].

Un modelo de comportamiento también podría incluir *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

[6] «Gráfica social» es un término que indica la visibilidad de amigos en los sitios de redes sociales y la capacidad para deducir rasgos de comportamiento a partir de los datos de estos amigos.

perfiles pueden ser utilizados para tomar decisiones que afecten significativamente a su propietario.

La tecnología de los dispositivos móviles inteligentes permite un control constante de los datos de localización. Los teléfonos inteligentes pueden captar permanentemente las señales procedentes de las estaciones de base y de puntos de acceso WiFi. Técnicamente, el seguimiento puede hacerse de forma secreta, sin informar al propietario, o también de forma semisecreta, cuando la persona «olvida» o no está adecuadamente informada de que los servicios de localización están activados o cuando los parámetros de accesibilidad de los datos sobre localización son cambiados de «privada» a «pública».

Aun cuando las personas permitan deliberadamente el acceso a sus datos de geolocalización en Internet, mediante servicios de rastreo y etiquetado geográfico, un acceso general e ilimitado crea nuevos riesgos que van desde la sustracción de datos hasta los robos en domicilios o incluso agresiones físicas y acoso.

Como ocurre con otras nuevas tecnologías, un riesgo importante del uso de datos de localización es la desviación de uso, el hecho de que, sobre la base de la disponibilidad de un nuevo tipo de datos, se desarrollen nuevos fines no previstos en el momento de la recogida de los datos.

## 4. Marco jurídico

El marco jurídico pertinente es la Directiva sobre protección de datos (95/46/CE), que se aplica en todos los casos de tratamiento de datos personales como resultado del tratamiento de datos de localización. La Directiva sobre la protección de la intimidad y las comunicaciones electrónicas (2002/58/CE, modificada por la Directiva 2009/136/CE) solo se aplica al tratamiento de datos de las estaciones de base por servicios y redes públicos de comunicación electrónica (operadores de telecomunicaciones).

### 4.1 Datos de estaciones de base tratados por operadores de telecomunicaciones

Los operadores de telecomunicaciones procesan continuamente datos de las estaciones de base en el marco de la prestación de servicios públicos de comunicaciones electrónicas[7]. También pueden procesarlos con el fin de prestar servicios de valor añadido. Este caso ya fue analizado por el Grupo de trabajo en el dictamen 5/2005 (WP115). Aunque algunos de los ejemplos del dictamen han quedado inevitablemente anticuados por la difusión de la tecnología de Internet y la incorporación de sensores en dispositivos cada vez más pequeños, las conclusiones y recomendaciones de dicho dictamen siguen siendo válidas en cuanto a la utilización de los datos de las estaciones de base.

[7] Téngase en cuenta que los puntos de acceso público WiFi ofrecidos por proveedores de telecomunicaciones también se consideran comunicaciones electrónicas y por lo tanto deberán en primer lugar ajustarse a las disposiciones de la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas.

1. Puesto que los datos sobre ubicación derivados de las estaciones de base se refieren a una persona física identificada o identificable, estarán sujetos a las disposiciones sobre protección de datos personales establecidas en la Directiva 95/46/CE, de 24 de octubre de 1995.
2. La Directiva 2002/58/CE, de 12 de julio de 2002 (revisada en noviembre de 2009 mediante la Directiva 2009/136/CE) es también aplicable, en virtud de la definición establecida en el artículo 2, letra c), de la misma:
*«'Datos de localización': cualquier dato tratado en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público».*

Si un operador de telecomunicaciones ofrece un servicio de geolocalización híbrido también basado en el procesamiento de otros tipos de datos de localización, como los GPS o WiFi, dicha actividad se considera como un servicio público de comunicaciones electrónicas. El operador de telecomunicaciones debe disponer del consentimiento previo de sus clientes si ofrece estos datos de geolocalización a terceros.

## 4.2 Datos procedentes de estaciones de base, WiFi y GPS tratados por prestatarios de servicios de la sociedad de la información

### 4.2.1 Aplicabilidad de la Directiva revisada sobre la protección de la intimidad y las comunicaciones electrónicas

Normalmente, las empresas que ofrecen servicios de localización y aplicaciones basadas en una combinación de datos de estaciones de base, GPS y WiFi son *servicios de la sociedad de la información* que, como tales, quedan explícitamente excluidos de la Directiva sobre la protección de la intimidad y las comunicaciones electrónicas, en virtud de la definición estricta de «servicio de comunicaciones electrónicas» (artículo 2, letra c), de la Directiva Marco revisada -sin modificaciones-)[8].

La Directiva sobre la protección de la intimidad y las comunicaciones electrónicas no se aplicará al tratamiento de datos de localización por los servicios de la sociedad de la información, incluso si dicho tratamiento se realiza a través de una red de comunicaciones electrónicas pública. Un usuario puede elegir entre transmitir los datos GPS a través de Internet, por ejemplo al acceder a través de Internet a servicios de navegación. En ese caso, la señal GPS se transmite en el nivel de aplicación de la comunicación en Internet, con independencia de la red GSM. El proveedor de servicios de telecomunicaciones actúa como mero transmisor: no puede acceder a

[8] Directiva 2002/21/CE, de 7 de marzo de 2002, artículo 2, letra c): «servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas».

datos GPS, WiFi o de estación de base comunicados desde y hacia un dispositivo móvil inteligente entre un usuario/abonado y un servicio de la sociedad de la información sin utilizar medios muy intrusivos como investigaciones en profundidad.

4.2.2 Aplicabilidad de la Directiva sobre protección de datos

Cuando no sea aplicable la Directiva revisada sobre la protección de la intimidad y las comunicaciones electrónicas, de conformidad con el artículo 1, apartado 2, de la Directiva 95/46/CE, «*Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1*».

En virtud del artículo 2.a) de la Directiva sobre protección de datos, los datos personales son «*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*».

El considerando 26 de la Directiva presta una especial atención a la expresión «identificable» cuando afirma 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*».

El considerando 27 de la Directiva esboza el amplio alcance de la protección: «[*considerando] que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión*».

En su dictamen 4/2007 sobre el concepto de datos personales, el Grupo de trabajo expuso unas amplias orientaciones sobre la definición de datos personales.

*Dispositivos móviles inteligentes*

Los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas. Generalmente, la posibilidad de identificación es directa e indirecta.

En primer lugar, el operador de telecomunicaciones que proporciona el acceso GSM y el acceso móvil a Internet suele tener un registro con el nombre, dirección y datos bancarios de cada cliente, en combinación con varios números únicos del dispositivo, como el IIEM/IMSI.

En segundo lugar, la compra de programas informáticos adicionales para el dispositivo (aplicaciones) requiere habitualmente un número de tarjeta de crédito y, por ende, enriquece la combinación del número (o números) único y datos de localización con datos identificativos directos.

La identificabilidad indirecta puede lograrse a través de la combinación del número (o números) único del dispositivo, en combinación con una o más ubicaciones calculadas.

Cada dispositivo móvil inteligente tiene como mínimo un identificador único, la dirección MAC. El dispositivo puede tener otros números de identificación únicos, añadidos por el creador del sistema operativo. Estos identificadores pueden ser transmitidos y tratados en el contexto de los servicios de geolocalización. Es un hecho que la ubicación de un dispositivo concreto puede calcularse de forma muy precisa, especialmente cuando se combinan las diferentes infraestructuras de geolocalización. Dicha localización puede referirse a una casa o a un empresario. Especialmente utilizando observaciones repetidas, es posible identificar al propietario del dispositivo.

Al considerar las medios disponibles de identificabilidad, debe tenerse en cuenta el factor de que las personas tienden a revelar cada vez más datos sobre localización personal en Internet, por ejemplo publicando la ubicación de su vivienda o de su lugar de trabajo en combinación con otros datos identificativos. Esta divulgación también puede suceder sin su conocimiento, cuando son localizadas geográficamente por otras personas. Esto permite vincular una pauta de localización o de comportamiento a un individuo concreto.

Además, tras el dictamen 4/2007 relativo al concepto de datos personales, también conviene destacar que un identificador único, en el contexto antes descrito, permite el seguimiento de un usuario de un dispositivo específico y, por tanto, permite individualizar al usuario, incluso si su verdadero nombre no es conocido.

*Puntos de acceso WiFi*

Esta forma indirecta de identificabilidad se aplica asimismo a los puntos de acceso WiFi[9]. La dirección MAC de un punto de acceso WiFi, en combinación con su ubicación calculada, está íntimamente ligada a la ubicación del propietario del punto de acceso.

Un responsable del tratamiento de datos razonablemente equipado puede calcular cada vez con mayor precisión la localización de un punto de acceso WiFi haciendo uso de la intensidad de la señal y de las actualizaciones de localización que estén efectuando los usuarios de sus servicios de geolocalización.

Con estos recursos, en muchos casos puede identificarse un pequeño grupo de apartamentos o casas en los que viviría el propietario del punto de acceso. La facilidad con la que será posible identificar a este titular de la dirección MAC dependerá del entorno:

- En zonas poco pobladas, en donde la dirección MAC apunta a una sola casa, el propietario de la residencia puede ser identificado directamente con herramientas como, por ejemplo, los registros del catastro, las páginas blancas telefónicas, los censos electorales o incluso un simple motor de búsqueda[10].
- En zonas más densamente pobladas y con ayuda de recursos como, por ejemplo, la intensidad de señal o la SSID (que cualquier persona con un dispositivo WiFi puede detectar), es posible determinar la localización precisa del punto de acceso y así, en muchos casos, la identidad de la persona que vive

[9] Los puntos de acceso WiFi incluso pueden ser directamente identificables, si el proveedor de acceso a Internet mantiene un registro de las direcciones MAC de los encaminadores WiFi que facilita a sus clientes identificados.

[10] La disponibilidad de estos censos o guías varía en función del Estado miembro.

en el lugar concreto (casa o apartamento) en el que está situado el punto de acceso.

- En zonas muy densamente pobladas, incluso contando con la ayuda de información sobre intensidad de la señal, la dirección MAC indicará varios apartamentos como posible localización del punto de acceso. En estas circunstancias, no es posible determinar con precisión y sin esfuerzo excesivo la identidad de la persona que vive en el apartamento en donde está situado el punto.

El hecho de que, en algunos casos, el propietario del dispositivo no pueda ser identificado en ese momento sin un esfuerzo no razonable, no obsta a la conclusión general de que la combinación de una dirección MAC de un punto de acceso WiFi con su ubicación calculada debe ser tratada como datos personales.

En estas circunstancias, y teniendo en cuenta que es improbable que el responsable del tratamiento de datos sea capaz de distinguir entre los casos en los que el propietario del punto de acceso WiFi es identificable y en los que no, el responsable deberá considerar todos los datos sobre encaminadores WiFi como datos personales.

Es importante recordar que no es necesario que la finalidad del tratamiento de estos datos de geolocalización sea identificar a los usuarios. El que ello requiera un esfuerzo irrazonable para identificar a los propietarios de los puntos de acceso WiFi está muy influenciado por las posibilidades técnicas de que disponga el responsable del tratamiento de datos o cualquier otra persona para identificarlos.

## 5. Obligaciones derivadas de la legislación sobre protección de datos

### 5.1 Responsable del tratamiento de datos

En el contexto de los servicios de geolocalización en línea prestados por servicios de la sociedad de la información pueden distinguirse tres diferentes funcionalidades, con distintas responsabilidades para el tratamiento de los datos personales. Se trata del responsable del tratamiento de datos de una infraestructura de geolocalización; el proveedor de una aplicación o un servicio específico de geolocalización; y el creador del sistema operativo de un dispositivo móvil inteligente. En la práctica, las empresas a menudo cumplen numerosas funciones al mismo tiempo, por ejemplo cuando combinan un sistema operativo con una base de datos que dispone de un inventario de puntos de acceso WiFi y una plataforma de publicidad.

#### 5.1.1 Responsables del tratamiento da datos de infraestructuras de geolocalización

Al igual que los operadores de telecomunicaciones cuando procesan la localización de un dispositivo específico con la ayuda de sus estaciones de base, los propietarios de bases de datos con un repertorio de puntos de acceso WIFI procesan datos personales al calcular la localización de un determinado dispositivo móvil inteligente. Puesto que ambos determinan los fines y medios de este tratamiento, son responsables del

tratamiento con arreglo a la definición del artículo 2, letra d), de la Directiva sobre protección de datos.

Es importante subrayar que el dispositivo concreto es fundamental para calcular su propia ubicación, al comunicar sus propios datos de localización (a menudo una combinación de GPS, WiFi y estación de base) y el identificador único de los puntos de acceso WiFi próximos al propietario de la base de datos[11]. Este dispositivo cumple también el criterio del artículo 4, apartado 1, letra c), de la Directiva sobre protección de datos, relativo a equipos situados en el territorio de un Estado miembro.

Como la dirección MAC de un punto de acceso WiFi, en combinación con su ubicación calculada, debe ser considerada como datos personales, la recogida de estos datos también resulta en el tratamiento de datos personales. Independientemente de la forma en que estos datos son recopilados (en un solo momento o de forma continua), el propietario de la base de datos debería cumplir las obligaciones de la Directiva sobre protección de datos.

### 5.1.2 Proveedores de aplicaciones y servicios de geolocalización

Los dispositivos móviles inteligentes permiten instalar programas informáticos de terceros, denominados «aplicaciones» y que pueden procesar los datos de localización (y otros) de un dispositivo móvil inteligente, independientemente del creador del sistema operativo o de los responsables del tratamiento de datos de la infraestructura de geolocalización.

Ejemplos de tales servicios son: un servicio de previsiones meteorológicas que establezca las posibilidades de lluvia en las próximos horas en una región muy específica, un servicio que ofrezca información sobre tiendas cercanas, un servicio de identificación de teléfonos perdidos o un servicio que muestre la ubicación de los amigos.

El proveedor de una aplicación que sea capaz de procesar datos de geolocalización es el responsable del tratamiento de datos personales resultantes de la instalación y uso de la aplicación.

Evidentemente, no siempre es necesario instalar programas informáticos inteligentes separados en un dispositivo móvil ya que a muchos servicios de geolocalización también se puede acceder a través de un navegador. Un ejemplo de tal servicio es la utilización de un mapa en línea por una persona que camina por la ciudad.

### 5.1.3 Creador del sistema operativo

El creador del sistema operativo del dispositivo móvil inteligente puede ser responsable del tratamiento de datos de geolocalización cuando interactúe directamente con el usuario y recoja datos personales (como, por ejemplo, al exigir un registro inicial del usuario o al recopilar información sobre localización a efectos de

[11] El dispositivo móvil puede transmitir los distintos datos de geolocalización que reciba con el fin de que el responsable del tratamiento pueda calcular su ubicación, o el propio dispositivo puede calcularla. En ambos casos, el dispositivo es un equipo esencial para el procesamiento.

mejorar sus servicios). Como responsable del tratamiento de datos, el creador deberá aplicar unos principios de diseño que respeten la intimidad con el fin de evitar un control secreto bien por el propio dispositivo o bien por las diferentes aplicaciones y servicios.

El creador es también el responsable del tratamiento de los datos que procesa si el dispositivo dispone de una función «llamar a casa». Puesto que en ese caso el creador decide los medios y el flujo de datos para tales fines, es el responsable del tratamiento de estos datos. Un ejemplo común de la funcionalidad «llamar a casa» es la adaptación automática a los husos horarios en función de la localización.

En tercer lugar, el creador es responsable del tratamiento de datos cuando ofrece una plataforma o alguna forma de venta de aplicaciones a través de la red y puede tratar los datos personales resultantes de la instalación y uso de las aplicaciones de geolocalización, con independencia de los proveedores de aplicaciones.

### 5.2 Responsabilidades de otras partes

Existen otras muchas partes en línea que permiten el tratamiento posterior de datos sobre ubicación tales como navegadores, sitios de redes sociales o medios de comunicación que permiten, por ejemplo el etiquetado geográfico. Cuando incorporan mecanismos de geolocalización en su plataforma, tienen la importante responsabilidad de decidir sobre los parámetros de la aplicación (activación o desactivación por defecto). Aunque solo son responsables del tratamiento en la medida en que procesen por sí mismos activamente datos personales, desempeñan un papel clave en la legitimación del tratamiento de datos por responsables del tratamiento de datos tales como los proveedores de aplicaciones específicas, por ejemplo en lo que se refiere a la visibilidad y calidad de la información sobre el tratamiento de datos.

### 5.3 Motivo legítimo

#### 5.3.1 Dispositivos móviles inteligentes

Si los operadores de telecomunicaciones quieren utilizar datos de la estación de base para prestar un servicio de valor añadido al cliente, con arreglo a la Directiva revisada sobre la intimidad y las comunicaciones electrónicas, deberán obtener su consentimiento previo. También deben asegurarse de que el cliente esté informado acerca de los términos de dicho procesamiento.

Dada la sensibilidad del procesamiento de los datos o pautas de datos de localización, el *consentimiento fundamentado previo* constituye también el principal factor aplicable para dar legitimidad al tratamiento de datos en lo que se refiere al procesamiento de las localizaciones de un dispositivo móvil inteligente en el contexto de servicios de la sociedad de la información.

Con arreglo a la Directiva sobre protección de datos (artículo 2.h), el consentimiento debe ser una manifestación de voluntad libre, específica e informada del interesado.

Según el tipo de tecnología utilizada, el dispositivo del usuario desempeña un papel relativamente activo en la transformación de los datos de geolocalización. El dispositivo es capaz de transmitir datos de localización procedentes de fuentes diferentes a cualquier tercero. Esta capacidad técnica no debe confundirse con la legalidad del tratamiento de dichos datos. Si los parámetros por defecto de un sistema operativo permiten la transmisión de datos de localización, la falta de intervención por parte de sus usuarios no debería confundirse con un consentimiento libremente otorgado.

En la medida en que los creadores de sistemas operativos y de otros servicios de la sociedad de la información procesan activamente datos de geolocalización (por ejemplo, cuando tienen acceso a información relativa a la ubicación desde el dispositivo o a través del mismo) también deben disponer del consentimiento fundamentado previo de sus usuarios. Debe quedar claro que este consentimiento no puede obtenerse libremente, haciendo obligatoria la aceptación de los términos y condiciones generales ni las posibilidades de exclusión voluntaria. Por defecto, los servicios de geolocalización deberían estar desactivados y los usuarios podrían consentir gradualmente la activación de aplicaciones específicas.

*Consentimiento de los empleados*

El consentimiento como fundamento del procesamiento legítimo es problemático en el mundo laboral. En su dictamen sobre el tratamiento de datos personales en el contexto laboral, el Grupo de Trabajo afirmó: «*Cuando se requiera el consentimiento de un trabajador y exista un perjuicio potencial o real relevante derivado de la falta de consentimiento, se considerará que el consentimiento no cumple lo establecido en el artículo 7 o en el artículo 8 si no es otorgado libremente. Si no es posible para el trabajador denegarlo, no se considerará consentimiento. (…) Un ámbito conflictivo se presenta cuando otorgar el consentimiento es una condición para el empleo. En teoría, el trabajador puede denegar su consentimiento, pero la consecuencia podría ser la pérdida de una oportunidad de empleo. En tales circunstancias el consentimiento no se otorga libremente y por tanto no es válido*»[12]. En vez de solicitar el consentimiento, los empresarios deben investigar si es una necesidad demostrable controlar la localización exacta de los empleados con un fin legítimo y sopesar dicha necesidad con los derechos y libertades fundamentales de los trabajadores. En los casos en que la necesidad pueda justificarse adecuadamente, la base jurídica podría ser el interés legítimo del responsable del tratamiento (artículo 7.f) de la Directiva sobre protección de datos). El empresario debe siempre buscar los medios menos intrusivos, evitar un seguimiento continuo y, por ejemplo, elegir un sistema que envíe una alerta cuando un empleado cruce una frontera virtual preestablecida. El empleado deberá poder desactivar cualquier dispositivo de vigilancia fuera de las horas de trabajo y deberá instruírsele sobre cómo hacerlo. Los dispositivos de seguimiento de vehículos no son dispositivos para la localización de empleados ya que su función es hacer un seguimiento o vigilar la ubicación de los vehículos en que estén instalados. Los empresarios no deben considerarlos como dispositivos para seguir o supervisar el comportamiento o el paradero de los conductores o de otro tipo de personal, por ejemplo, mediante el envío de alertas relacionadas con la velocidad del vehículo.

[12] WP48, Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral.

*Consentimiento de los niños*

En algunos casos, el consentimiento del niño debe ser dado por sus padres o representantes legales. Esto significa, por ejemplo, que el proveedor de una aplicación de geolocalización debe informar a los padres sobre la obtención y el uso de datos de geolocalización y obtener su consentimiento, antes de recabar y procesar información sobre sus hijos. Algunas aplicaciones de geolocalización están específicamente diseñadas para el control parental, por ejemplo informando continuamente sobre la localización del dispositivo en un sitio Internet o mediante la emisión de una alerta si el dispositivo sale de un territorio predefinido. El uso de este tipo de aplicaciones es problemático. En su Dictamen 2/2009[13] sobre la protección de los datos personales el Grupo de Trabajo del Artículo 29 afirmó: *«Hay que evitar en todo caso que, por motivos de seguridad, los niños sean sometidos a una vigilancia excesiva que limite su autonomía. En este contexto, hay que alcanzar un equilibrio entre la protección de la intimidad y la vida privada de los niños y su seguridad»*.

El marco jurídico establece que los padres son responsables de que se garantice el derecho de los niños a la intimidad. Como mínimo, si los padres consideran que la utilización de dicha aplicación está justificada en circunstancias específicas, los niños deberán ser informados y, tan pronto como sea razonablemente posible, deberá permitírseles participar en la decisión de utilizarla.

El consentimiento debe ser específico para cada uno de los distintos fines para los que se procesan los datos. El responsable del tratamiento de datos deberá indicar claramente si su servicio se limita a responder a la pregunta voluntaria «¿Dónde me encuentro ahora mismo?» o si su finalidad es responder a las preguntas «¿Dónde estás, dónde has estado y dónde estarás la próxima semana?». En otras palabras, el responsable del tratamiento deberá prestar una atención específica al consentimiento para fines no esperados por el interesado como, por ejemplo, la elaboración de perfiles o la orientación del comportamiento.

Si la finalidad del tratamiento cambia sustancialmente, el responsable del tratamiento deberá recabar la renovación del consentimiento específico. Por ejemplo, si inicialmente una empresa declaró que no comunicaría datos personales a ningún tercero, pero ahora desea compartirlos, deberá contar con el consentimiento previo de cada cliente. Una falta de respuesta (o cualquier otro tipo de modalidad de desistimiento) no es suficiente.

Es importante distinguir entre consentimiento ante un servicio esporádico y autorización para una suscripción. Por ejemplo, a fin de utilizar un servicio de geolocalización particular, puede ser necesario activar dichos servicios en el dispositivo o navegador. Si esta capacidad de geolocalización se activa, cualquier sitio Internet puede leer los detalles de localización del usuario del dispositivo móvil inteligente. Con el fin de prevenir los riesgos de vigilancia secreta, el Grupo del artículo 29 considera esencial que el dispositivo advierta continuamente de que la geolocalización está activada, por ejemplo a través de un icono visible de forma permanente.

[13] WP 160, Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas).

El Grupo de trabajo recomienda que los proveedores de aplicaciones o servicios de geolocalización renueven la autorización individual (incluso si no hay cambio en la naturaleza del procesamiento) tras un período adecuado. Por ejemplo, no sería adecuado continuar con el procesamiento de datos de localización cuando un individuo no haya utilizado activamente el servicio durante los 12 meses anteriores. Incluso cuando una persona haya utilizado el servicio, se le debería recordar al menos una vez al año (o más a menudo, cuando la naturaleza del tratamiento así lo exija), la naturaleza del tratamiento de sus datos personales y ofrecerle un medio sencillo para excluirse.

Por último, pero no menos importante, los interesados deberán poder retirar su consentimiento de forma muy fácil, sin consecuencias negativas para el uso de su dispositivo. Independientemente de las Directivas europeas de protección de datos, el World Wide Web Consortium (W3C) ha desarrollado un proyecto de norma API de geolocalización que subraya la necesidad de consentimiento previo, expreso e informado[14]. El W3C explica en concreto la necesidad de respetar la retirada del consentimiento, aconsejando a los implantadores de la norma que consideren que «*el contenido almacenado en una determinada URL cambia de tal forma que las autorizaciones de localización concedidas anteriormente ya no se aplican en lo que concierne al usuario. O los usuarios pueden simplemente cambiar de idea*».

*Ejemplo de mejores prácticas para proveedores de aplicaciones de geolocalización*

| |
|---|
| La aplicación que desee utilizar datos de geolocalización informará claramente al usuario sobre los fines para los que quiere utilizarlos y solicitará su consentimiento inequívoco para cada una de las posibles finalidades distintas. El usuario elegirá activamente el nivel de la geolocalización (por ejemplo, a escala de un país, ciudad, código postal o con la mayor precisión posible). Una vez que el servicio de localización se active, un icono estará permanentemente visible en cada pantalla indicando dicha activación. El usuario podrá retirar su consentimiento en cualquier momento y sin tener que abandonar la aplicación y también podrá suprimir, fácil y permanentemente, cualquier dato de localización almacenado en el dispositivo. |

### 5.3.2 Puntos de acceso WiFi

En virtud de la Directiva sobre protección de datos, las empresas pueden tener un interés legítimo en la necesaria recopilación y tratamiento de las direcciones MAC y de las localizaciones calculadas de los puntos de acceso WiFi para el fin específico de ofrecer servicios de geolocalización.

El interés legítimo del artículo 7.f) de la Directiva sobre protección de datos exige un equilibrio entre el interés legítimo del responsable y los derechos fundamentales de los interesados. Dada la naturaleza semiestática de los puntos de acceso WiFi, la cartografía de dichos puntos constituye, en principio, una menor amenaza para la intimidad de los propietarios de estos puntos que el seguimiento instantáneo de la ubicación de los dispositivos móviles inteligentes.

El equilibrio entre los derechos del responsable del tratamiento de datos y los derechos del interesado es dinámico. Para que los intereses legítimos de los

[14] W3C, Geolocalización API: http://www.w3.org/TR/geolocation-API/

responsables del tratamiento prevalezcan en el tiempo sobre los correspondientes a los interesados, deben desarrollar y aplicar garantías tales como el derecho a poder abandonar fácil y permanentemente la base de datos, sin necesidad de proporcionar a la entidad responsable del tratamiento datos personales complementarios para dicha base. Los responsables del tratamiento pueden, por ejemplo, usar programas informáticos para detectar automáticamente que una persona está conectada a un determinado punto de acceso[15].

Además, con el fin de ofrecer servicios de geolocalización, la recogida y procesamiento de SSID no es necesaria y por lo tanto es excesiva a efectos de ofrecer servicios basados en la localización en mapas de los puntos de acceso WiFi.

### 5.4 Información

Los distintos responsables del tratamiento de datos deben asegurarse de que los propietarios del dispositivo móvil inteligente estén adecuadamente informados sobre los elementos clave del tratamiento, de conformidad con el artículo 10 de la Directiva sobre protección de datos, tales como la identidad del responsable del tratamiento; la finalidad del tratamiento; el tipo de datos; la duración del tratamiento; los derechos de los titulares de los datos a acceder, rectificar o suprimir sus datos; y el derecho a retirar su consentimiento.

La validez del consentimiento está vinculada indisolublemente a la calidad de la información sobre el servicio. La información debe ser clara, completa, comprensible para un público amplio y no técnico, y accesible permanente y fácilmente.

La información debe estar destinada a un público amplio. Los responsables del tratamiento no pueden suponer que sus clientes son personas técnicamente cualificadas solo porque posean un dispositivo móvil inteligente. La información deberá estar adaptada a la edad si el responsable del tratamiento sabe que atrae a un público juvenil.

Si los proveedores de aplicaciones de geolocalización pretenden calcular la localización de un dispositivo más de una vez, deben mantener a su clientela informada siempre que procesen datos sobre localización. Asimismo, deben permitir a sus clientes renovar o revocar su consentimiento. Con el fin de alcanzar estos objetivos, los proveedores de las aplicaciones deberán colaborar estrechamente con el creador del sistema operativo. El creador es técnicamente el mejor situado para crear

---

[15] Un posible caso de uso es el siguiente:

1. Un interesado va a una página de Internet específica, a través de la cual puede entrar en la dirección MAC de su punto de acceso WiFi.
2. Si la dirección MAC figura en la base de datos con los puntos de acceso WiFi cartografiados, el responsable del tratamiento de los datos puede mostrar una página de verificación que contenga un texto que solicite la tabla ARP del dispositivo de Internet. En teoría, las direcciones MAD de la WLAN pueden mostrarse mediante la orden «ARP -a». Con ayuda del código contenido en el navegador, por ejemplo el Java, esta tabla ARP puede reproducirse en el fondo.
3. Si la dirección MAC no aparece en la tabla ARP, se determina que el usuario conectado a la WLAN es también el que accede a la dirección MAC de la WLAN local. Así pues, el responsable del tratamiento verifica la solicitud de supresión de datos personales de una forma fácil y automática.

una advertencia permanente visible de que los datos de localización están siendo procesados. El creador también es el mejor situado para verificar que no se ofrezcan secretamente aplicaciones que controlen el paradero de los dispositivos móviles inteligentes.

Si el creador del sistema operativo ha creado una funcionalidad «llamar a casa» u otros medios de acceso a los datos almacenados en el dispositivo, o si tiene acceso de otra forma a datos de localización, por ejemplo a través de anunciantes de terceros, deberá informar previamente al interesado sobre los fines (específicos y legítimos) para los que desea procesar estos datos y la duración del tratamiento.

La obligación de informar a las personas afectadas se aplica también a los responsables del tratamiento de las bases de datos con puntos de acceso WiFi geolocalizados, que deberán informar adecuadamente al público en general sobre su identidad y la finalidad del tratamiento de datos y comunicar cualquier otra información pertinente. Una mera mención de la posible recogida de datos sobre puntos de acceso WiFi en una declaración específica de privacidad dirigida a los usuarios de una aplicación de geolocalización no es suficiente. Existen medios suficientes, en línea como fuera de línea, para informar al gran público.

### 5.5 Derechos de los interesados

Los interesados tendrán derecho a obtener de los distintos responsables del tratamiento acceso a los datos de localización que hayan recogido de sus dispositivos móviles inteligentes, así como información sobre los fines del tratamiento y de los destinatarios o categorías de destinatarios a quienes se comuniquen los datos. La información deberá proporcionarse en un formato legible por personas, es decir, mediante puntos geográficos, en vez de mediante números abstractos como, por ejemplo, los relativos a estaciones de base.

Los interesados también tendrán derecho a acceder a posibles perfiles sobre la base de estos datos de localización. Si se guarda información sobre localización, los usuarios deberán poder actualizar, rectificar o suprimir esta información.

El Grupo de trabajo recomienda que los responsables del tratamiento de datos busquen formas seguras de facilitar el acceso directo en línea a datos de localización y posibles perfiles. Es fundamental que tal acceso se ofrezca sin solicitar datos personales adicionales para determinar la identidad del interesado.

### 5.6 Períodos de retención

Los proveedores de servicios de geolocalización y de aplicaciones deben determinar un período de retención de datos de localización no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Deberán garantizar que los datos de geolocalización, o los perfiles obtenidos a partir de estos datos, sean suprimidos después de un período justificado.

En caso de que se pueda demostrar la necesidad para el creador del sistema operativo o el responsable de una infraestructura de geolocalización de recoger datos sobre geolocalización a efectos de actualizar o mejorar su servicio, deberá velarse cuidadosamente por evitar que estos datos puedan ser (indirectamente) identificables. En particular, incluso si el dispositivo móvil se identifica mediante un dispositivo identificador único (UDID) asignado al azar, este número único solo deberá almacenarse durante un período máximo de 24 horas a efectos operativos. Transcurrido este plazo, este UDID deberá volver a ser nuevamente anónimo, teniendo en cuenta al mismo tiempo que la anonimización real es cada vez más difícil de llevar a cabo y que la combinación de datos sobre ubicación podría dar como resultado finalmente la identificación. Dicho UDID no debería poder ser asociado a anteriores o futuros UDID atribuidos al producto, ni tampoco a cualquier identificador fijo del usuario o al teléfono (tales como dirección MAC, número IIEM/IMSI o cualquier otro número de cuenta).

Con respecto a los datos sobre puntos de acceso WiFi, una vez que la dirección MAC de un punto de acceso WiFi está asociada a una nueva localización, sobre la base de la continua observación de los propietarios de dispositivos inteligentes móviles, la localización anterior deberá ser suprimida inmediatamente con objeto de impedir cualquier utilización posterior de los datos con fines inadecuados, como actividades de mercadotecnia dirigidas a personas que han cambiado su localización.

## 6. Conclusiones

Con la ayuda de tecnologías de geolocalización como las estaciones de bases de datos, el GPS y el cartografiado de puntos de acceso WiFi, los dispositivos móviles inteligentes pueden ser seguidos por todos los tipos de responsables del tratamiento de datos, para fines que van desde la publicidad orientada por los comportamientos al control de los hijos.

Puesto que los teléfonos inteligentes y las tabletas digitales están inextricablemente vinculados a su propietario, las pautas de desplazamiento de los dispositivos ofrecen una visión muy precisa de la vida privada de los propietarios. Uno de los grandes riesgos es que los propietarios no se percaten de que están transmitiendo su localización y a quién. Otro riesgo vinculado es que el consentimiento para determinadas aplicaciones que utilicen sus datos de localización no sea válido, ya que la información sobre los elementos clave del procesamiento es incomprensible, anticuada o insuficiente por cualquier otro motivo.

Existen diferentes obligaciones impuestas a las distintas partes interesadas, desde los creadores de los sistemas operativos a los proveedores de aplicaciones y a partes como las redes sociales que insertan funcionalidades de localización para dispositivos móviles en sus plataformas.

### 6.1 Marco jurídico

- El marco jurídico de la UE para el uso de los datos de geolocalización procedentes de dispositivos móviles inteligentes es fundamentalmente la Directiva sobre protección de datos. Los datos de localización procedentes de dispositivos móviles inteligentes son datos personales. La combinación de la

dirección MAC única y la localización calculada de un punto de acceso WiFi debe ser tratada como datos personales.

- Además, la Directiva 2002/58/CE revisada, sobre la protección de la intimidad y las comunicaciones electrónicas, se aplica únicamente al tratamiento de datos de la estación de base por operadores de telecomunicaciones.

6.2 Responsables del tratamiento de datos

- Pueden distinguirse tres tipos de responsables del tratamiento de datos: responsables del tratamiento de infraestructuras de geolocalización (en particular los responsables del cartografiado de puntos de acceso WiFi), proveedores de aplicaciones y servicios de geolocalización, y creadores del sistema operativo de dispositivos móviles inteligentes.

6.3 Interés legítimo

- Debido a que los datos de localización de los dispositivos móviles inteligentes revelan detalles íntimos sobre la vida privada de su propietario, el principal interés legítimo aplicable es el consentimiento fundamentado previo.
- El consentimiento no puede obtenerse a través de condiciones generales.
- El consentimiento debe ser específico para los diferentes fines para los que se procesen los datos, por ejemplo para elaborar perfiles y orientaciones de comportamiento. Si la finalidad del tratamiento de los datos cambia de forma sustancial, el responsable del tratamiento deberá obtener la renovación del consentimiento específico.
- Por defecto, los servicios de localización deben estar desconectados. Un posible mecanismo de exclusión voluntaria no constituye un mecanismo adecuado para obtener el consentimiento del usuario informado.
- El consentimiento es problemático en el caso de los trabajadores asalariados y los niños. Por lo que respecta a los trabajadores, los empresarios solo podrán adoptar esta tecnología cuando sea una necesidad demostrable para un fin legítimo y el mismo objetivo no pueda ser alcanzado con medios menos intrusivos. Por lo que respecta a los niños, los padres deben juzgar si la utilización de dicha aplicación está justificada en circunstancias específicas. Como mínimo, deberán informar a sus hijos y, tan pronto como sea razonablemente posible, les permitirán participar en la decisión de utilizar dicha aplicación.
- El Grupo de trabajo recomienda limitar el período de validez de la autorización y recordar su existencia a los usuarios al menos una vez al año. Recomienda igualmente una claridad suficiente en el consentimiento con respecto a la precisión de los datos de localización.
- Los interesados deberán poder retirar su consentimiento de forma muy fácil, sin consecuencias negativas para el uso de su producto.
- Con respecto a la cartografía de puntos de acceso WiFi, las empresas pueden tener un interés legítimo en la necesaria recogida y tratamiento de direcciones MAC y las localizaciones calculadas de los puntos de acceso WiFi para el fin específico de prestación de servicios de geolocalización. El balance de intereses entre los derechos del responsable del tratamiento de datos y de los afectados exige que el responsable del tratamiento ofrezca el derecho a borrarse fácil y permanentemente de la base de datos, sin solicitar datos personales adicionales.

6.4 Información

- La información deberá ser clara, completa, comprensible para un público amplio y no técnico, y accesible de forma permanente y fácil. La validez del consentimiento está vinculada indisolublemente a la calidad de la información sobre el servicio.
- Los terceros, como los navegadores y los sitios de redes sociales, deben desempeñar un papel clave en lo que se refiere a la visibilidad y la calidad de la información sobre el tratamiento de los datos de geolocalización.

6.5 Derechos de los interesados

- Los distintos responsables del tratamiento de información de geolocalización procedente de dispositivos móviles deben permitir a sus clientes acceder a sus datos de localización en un formato legible por personas y permitir la rectificación y el borrado sin recoger datos personales excesivos.
- Los interesados también tendrán derecho de acceso, rectificación y borrado de posibles perfiles basados en estos datos de localización.
- El Grupo de trabajo recomienda la creación de un acceso en línea (seguro).

6.6 Períodos de retención

- Los proveedores de aplicaciones o servicios de geolocalización deberán aplicar políticas de retención que garanticen que los datos de geolocalización o los perfiles obtenidos a partir de estos datos, sean suprimidos después de un período justificado.
- Si el creador del sistema operativo o el responsable del tratamiento de la infraestructura de geolocalización procesa un número único, tal como una dirección MAC o UDID en relación con datos de localización, este número único de identificación solo podrá almacenarse durante un período máximo de 24 horas, con fines operativos.

Hecho en Bruselas,
el 16 de mayo de 2011

*Por el Grupo de trabajo*
*El Presidente*
*Jacob KOHNSTAMM*