Fecha de recepción: 27 de junio de 2016 / Fecha de aprobación: 2 de octubre de 2016

EL USO DE SISTEMAS DE LOCALIZACIÓN EN LAS PLATAFORMAS DE COMUNICACIÓN EN LÍNEA O EN LAS REDES SOCIALES

JUAN CAMILO CASTELLANOS MEJÍA
LUIS ALBERTO MONTEZUMA CHÁVEZ

Artículo de reflexión

DOI: http://dx.doi.org/10.15425/redecom.16.2016.05

Universidad de los Andes
Facultad de Derecho
Rev. derecho comun. nuevas tecnol. No. 16
julio - diciembre de 2016. e-ISSN 1909-7786

El uso de sistemas de localización en las plataformas de comunicación en línea o en las redes sociales

Resumen

El crecimiento de las redes sociales que utilizan sistemas basados en localización (LBSN, por sus siglas en inglés), claramente justifica la necesidad de la industria y de las autoridades de protección de datos de empezar a regular, mediante diferentes herramientas, el tratamiento de los datos personales de localización. El presente trabajo examina los diferentes sistemas basados en localización y cómo las plataformas los utilizan, con el propósito de presentar una serie de recomendaciones a las redes sociales, para que puedan cumplir con el régimen de protección de datos establecido en la Ley 1581 de 2012.

Palabras clave: datos personales, servicios de geolocalización, infraestructuras de geolocalización, riesgos en la privacidad, servicios de redes sociales, responsable del tratamiento.

The use of localization systems in online communication platforms or social networks

Abstract

The growth of Location Based Social Networks (LBSN), clearly justify the need for the industry and DPA to start using different mechanisms to regulate the processing of location personal data. For that motive, this paper examines the different location-based systems and how those platforms use it, in order to present a series of recommendations to the social networks, so they can comply with the data protection regime establish in the Law 1581 2012.

Keywords: Personal Data, Geolocation services, Geolocation Infrastructures, Privacy Risks, Social Network Service (SNS), Controller.

El uso de sistemas de localización en las plataformas de comunicación en línea o en las redes sociales*

JUAN CAMILO CASTELLANOS MEJÍA[1]
LUIS ALBERTO MONTEZUMA CHÁVEZ[2]

SUMARIO

* Cómo citar este artículo: Castellanos Mejía, J. C. y Montezuma Chávez, L. A. (Diciembre, 2016). El uso de sistemas de localización en las plataformas de comunicación en línea o en las redes sociales. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías,* (16). Universidad de los Andes (Colombia). http://dx.doi.org/10.15425/redecom.16.2016.05

1. Abogado, Universidad de los Andes. LL.M in Information & Communication Technology, Universidad de Oslo. Magíster en Derecho Económico, Universidad Javeriana. Correo: nefto1234@gmail.com.

2. Abogado, Universidad Libre. Especialista en Legislación Financiera y magíster en Derecho Privado, Universidad de los Andes. Magíster en Protección de Datos, Transparencia y Acceso a la Información, Universidad CEU San Pablo. Correo: luismontezumachavez@gmail.com.

Introducción

Muchas personas se han preguntado por qué cuando acceden a una página web o a una aplicación móvil —entre ellas a las redes sociales—, la información relacionada con su ubicación es rastreada sin que, frente a este caso en particular, el proveedor de la plataforma web o de la red social cuente con el consentimiento, previo, expreso e informado del usuario. Al respecto, en una investigación llevada a cabo por la Autoridad de Protección de Datos de Alemania, se encontró que Google recolectaba y almacenaba los datos de las redes locales wi-fi de los edificios que fotografiaba a través de su servicio Street View sin conocimiento de los residentes (*El País*, 29 de abril de 2010), circunstancia que se está replicando en otros sitios en línea.

Como prueba de lo anterior, el diario *El País* de España, en una columna publicada en marzo del 2010, reportó que Twitter permite a sus usuarios compartir con sus seguidores la información relacionada con su localización geográfica, sin que, según se deduce, la red social contara con el consentimiento de los usuarios titulares. Es decir, que las personas pueden ser ubicadas desde el lugar donde suben un tweet y, a su vez, compartir esa información con su comunidad. "El sistema funciona con base en la dirección IP del ordenador del internauta y los puntos de acceso inalámbrico más cercanos y obtiene una estimación de la ubicación del internauta" (*El País*, 2010, párr. 2).

Otros casos particulares frente al uso de la localización por parte de las plataformas de redes sociales son los siguientes: (i) Snapchat transmite información de localización de sus usuarios a su aplicación Android, a pesar de que su política de privacidad señala que esa red social no rastrea a sus usuarios ni accede a dicha información (Citron, 2014); (ii) WhatsApp necesita acceder a la locación del teléfono móvil del usuario para que este pueda compartir su ubicación con sus contactos; (iii) Facebook recolecta la posición geográfica específica obtenida a través de señales de sistemas de posicionamiento global (Global Positioning System –GPS), bluetooth o wifi, "para personalizar [sus] servicios para cada persona, por ejemplo, para [ayudarla] a registrar una visita y encontrar eventos locales u ofertas en [su] zona, o bien para avisarles a [sus] amigos que te encuentras cerca" (Facebook, 2015, párr. 4, Cómo usamos...). Por lo tanto, es un hecho indiscutible que Facebook almacena información de la ubicación geográfica de un individuo (Lee, 2007, p. 1).

Del mismo modo, Apple utiliza una combinación de datos móviles, wifi, bluetooth y GPS para determinar la ubicación de sus clientes y, de paso, activa los siguientes servicios del sistema basados en la ubicación: (i) tráfico; (ii) populares cerca; (iii) ubicaciones frecuentes; (iv) iAds según la ubicación; (v) sugerencias de spotlight; (vi) avisos basados en la ubicación; (vii) compartir la ubicación del usuario. Asimismo, en el documento "Pensamientos Universitarios" se precisa: "Si no te encuentras dentro de la línea de visión de los satélites GPS, tu dispositivo puede determinar tu localización utilizando localizaciones masivas de Wi-Fi y torres

de telefonía móvil o iBeacons" (Domínguez, 2014, qué pasos... párr. 1).

Los anteriores ejemplos son una prueba clara de que los proveedores de servicios de redes sociales cuentan con técnicas o herramientas que identifican fácilmente la posición exacta de una persona que accede a su perfil o servicios, escribe un comentario, envía un mensaje o transmite esa información a otras plataformas electrónicas, con el fin de elaborar perfiles publicitarios.

En una columna publicada en el diario *El País*, en marzo de 2010, se hizo referencia a que "esta información sirve al suministrador de publicidad o contenidos personalizados para localizar con más precisión dónde se halla el cliente. Para ello debe tener localizadas estas redes particulares" (p. 1). En este punto tenemos que "en el mercado hindú de telecomunicaciones las aplicaciones Android han utilizado explícitamente los datos de ubicación con el único fin de introducir publicidad en la pantalla de cada dispositivo" (Payeras Capellá, Mut Puigserver, Paniza Fullana e Isern Deyà, 2014, p. 82). Lo que significa, en otras palabras, que un proveedor de redes sociales puede identificar el gusto de una persona respecto de una marca específica de ropa, con base en la información de cuántas veces ha estado esta persona en el sitio, y remitirle publicidad de la marca al momento en que se encuentre alrededor del almacén. Esto es llamado "geomarketing".

El Grupo de Trabajo del Artículo 29 (en adelante GT 29), en el Informe de trabajo 185 (Opinión 13/2011, p. 7) indicó que tener conocimiento de la posición geográfica de una persona

> permite a los proveedores de servicios basados en la geolocalización tener una visión más íntima de los hábitos y patrones de los propietarios de los datos de un dispositivo y construir perfiles extensos. De un patrón de inactividad en la noche, el lugar de dormir puede ser deducido, y de un patrón regular de viajes en la mañana, la localización de un empleado podría ser deducida. El perfil puede incluir la información derivada del movimiento de los patrones de movimiento de amigos, basados en el llamado gráfico social.[3]

En esa misma línea de análisis, Philip Nolan y Oison Tobin ponen de manifiesto: "La tecnología de geolocalización tiene un potencial de comercio inmenso para las organizaciones. La capacidad para adaptar servicios y anuncios al paradero exacto de un usuario representa un gran salto para la comercialización" (2011, p. 7). Así mismo, dice Alexandra D. Vesalga, citando a Dan Tyna:

> Los datos de geolocalización —datos que señalan la ubicación de un usuario— son uno de los datos más útiles, vitales y codiciados por las compañías tecnológicas, en la medida en que permiten a un servicio web hacer

3. Aclaramos que la mayoría de las citas textuales son traducciones no oficiales del inglés al español, realizadas por los autores del presente artículo.

> sugerencias relevantes basadas en una locación en tiempo real de un usuario y mejorar así la publicidad en línea dirigida. (2013, p. 460).

Para una mayor claridad al respecto: con la información recolectada en los perfiles, Facebook puede inferir que los *fans* tienen interés y actitud positiva acerca de una marca, pero la publicidad basada en la localización puede entregar información en tiempo real e histórico de los productos o servicios adquiridos, lo que se traduce en resultados reales de las preferencias de los clientes (Olenski, 2013), como dónde se encuentra un usuario comprando y comiendo. Es claro que la posición geográfica es vital para ofrecer con mayor precisión bienes, productos y servicios, de acuerdo con las necesidades de los clientes.

No obstante lo anterior, se señala en el informe de Isaca (*Information Systems Audit and Control Association)*:

> Información de un GPS y etiquetas de geolocalización, en combinación con otra información personal, puede ser utilizada por criminales para identificar la ubicación presente o futura de un individuo, facilitando de esa manera la capacidad de causarle daño a este o a su propiedad, en actos que van desde robo, hurto y acecho hasta el secuestro y la violencia doméstica. (2011, p. 8).

De igual manera, Isaca indica: "La geolocalización puede dar una ventaja competitiva a los rivales en el negocio" (2011, p. 9).

Por otro lado, para Roger Clarke, "la mayoría de las técnicas de localización personal se limitaban a establecer dónde la persona vivía o trabajaba" (2000, 2.2. Definitions, p. 2). Sin embargo, en la actualidad, como lo señalan Cottrill y Thakuriah, en "Privacy in context: an evaluation of policy-based approaches to location privacy protection", el rápido crecimiento basado en la localización y las tecnologías móviles ha llevado a un aumento masivo en la cantidad de información de un individuo (2014, p. 179), "haciendo posible (...) poder examinar varios aspectos de la vida de otras personas" (Cheung, 2014, p. 43). Agrega Cheung lo siguiente: "Al detectar que una persona visita una mezquita cada semana, nosotros podemos ser capaces de inferir su probable filiación religiosa" (2014, p. 6). Por lo tanto, con un patrón de movilidad geográfica se puede inferir, fácilmente, el lugar de nacimiento de una persona, su origen racial, su orientación sexual, su creencia religiosa, su vocación política, entre otro tipo de información catalogada como sensible.

Igualmente, Payeras Capellá et al. precisan:

> La información de localización irá acompañada de una información asociada que dependerá de la configuración del usuario. Por ejemplo, podrá incorporar los últimos detalles sobre tráfico, clima, sitios de interés, disponibilidad de ciertos servicios dentro de la ciudad, ayuda a la navegación o con antecedentes históricos y económicos, etc. (2014, p. 80).

Las plataformas tecnológicas capturan, almacenan y analizan en todas sus posibles formas

la ubicación de una persona en un punto concreto en el espacio, "que se mide en coordenadas de latitud (x), longitud (y) y altura (z)" (Beltrán López, 2012, p. 25), y en tiempo real, para "localizarlo en el mapa con una alta precisión en un punto dado en el tiempo" (Isaca, 2011, p. 5). Dijo Roger Clarke: "El 'espacio' en el que se realiza un seguimiento de ubicación de una entidad es generalmente físico o geográfico, pero puede ser virtual, la interacción de una persona con una organización particular" (2000, 2.2. Definitions, párr. 4). Esto incluye, igualmente, el lugar donde aparentemente estará la persona en un futuro. En este contexto resulta evidente que, a primera vista, los sistemas de geolocalización conocen los movimientos habituales de una persona en el pasado y presente, así como el rastro o itinerario de todas sus ubicaciones en un futuro.

En todo caso, como lo señalan Diane Gan y Lily R. Jenkins,

> la información de geolocalización puede ser recogida de muchas maneras diferentes; con las fotografías se proporcionan la mayoría de ese tipo de datos. En efecto, con las nuevas cámaras los datos de geolocalización se recaban automáticamente con respecto a dónde se tomó la foto, y después se almacenan dentro del metadato EXIIF (Exchangeable Image File Format) registros de la imagen. (2015, p. 71).

Así, Instagram permite subir una fotografía con las coordenadas geográficas del lugar donde fue tomada. Según Fernando Camperos:

> Esto permitirá que las fotos pasen a formar parte del gran conjunto de imágenes tomadas en aquel mismo lugar. Si tomas fotos en sitios públicos, como un parque, un centro de eventos, un concierto o un punto de atractivo turístico, el haber incluido el lugar donde la tomaste te permitirá ver fácilmente las fotos que otros usuarios han tomado en el mismo lugar y que son públicas. Estas fotos, con sus coordenadas geográficas, también pasarán a engrosar tu mapa personal con fotos de Instagram, el que te permitirá revisar una y otra vez esos lugares que ya has explorado. (s.f., párr. 5).

Ahora bien, son ejemplos de técnicas que se utilizan para localizar a un usuario: (i) geolocalización basada en direcciones de protocolo de Internet —direcciones IP— geolocation by IP Address; (ii) geolocalización mediante redes wifi —Geolocation from Wi-Fi Networks—; (iii) geolocalización basada en Cell-ID —Geolocation by Cell Tower Triangulation—; (iv) sistema de posicionamiento global –GPS; y, (iv) Manual Input (Doty, Mulligan y Wilde, 2010, p. 12).

En ese orden de ideas, el presente escrito explica, en primer lugar, si la información relacionada con la posición geográfica de un individuo puede ser catalogada como dato personal. Para lograr lo anterior se trae a colación qué se entiende por *dato personal*. Este criterio es clave para establecer, si de la ubicación de un vehículo se puede determinar la posición geográfica de una persona física.

En segundo lugar, y no menos importante que lo anterior, dejar definido el concepto sistemas

de localización, también llamados en algunos documentos *sistemas de geolocalización*.

Y, finalmente, se llama la atención sobre la necesidad de que los proveedores de servicios de redes sociales se adhieran de manera vinculante y obligatoria a códigos de buenas prácticas, que deberían incluir medidas de ejecución eficaces y sanciones disciplinarias (GT 29, 2009, p. 13). Ello les permitiría, como se explica en el último capítulo del presente escrito, ser transparentes con sus usuarios frente al uso de la información recolectada, y que se relaciona con su posición geográfica, resaltando la obligación de contar con su consentimiento para llevar a cabo el tratamiento de datos personales.

I. EL TRATAMIENTO DEL DATO DE LOCALIZACIÓN

Este capítulo tiene como objetivo primordial determinar si la ubicación de una persona es catalogada como información de carácter personal. La respuesta al anterior planteamiento jurídico depende del concepto puro y simple de dato personal, en particular cuando se habla de aquella información relativa a un sujeto identificado o identificable. La forma escogida para explicarlo permite, como se podrá observar en párrafos posteriores, concluir que toda información concerniente a la posición geográfica de un individuo es, por regla general, dato personal y, por consiguiente, está sujeta al ámbito de aplicación del Régimen de Protección de Datos Personales.

A. Algunos aspectos sobre la definición de dato personal

El dato personal es aquella pieza de información relativa a una persona identificada o identificable. Precisa Ana Isabel Herrán Ortiz lo siguiente:

> Siguiendo con la definición que acoge la Directiva de 'dato personal', para que efectivamente el tratamiento de un dato se encuentre en el ámbito de aplicación de aquella deberá reunir dos condiciones: una, que se trate de un dato personal, relativo a la persona física; y dos, que la información o el dato se refiera a una persona identificada o identificable. (2002, p. 126).

Por su parte, Mónica Vilasau Solana, haciendo referencia a la Ley Orgánica Española de Protección de Datos, indica que el Régimen de Protección de Datos

> resulta aplicable a cualquier dato, con independencia de su relevancia, incluso si se trata de datos que no inciden en la esfera de intimidad de la persona ya que mediante datos irrelevantes se puede obtener información íntima y trazar perfiles psicológicos de los sujetos (...) Hay que volver a la idea inicial según la que [sic] para que exista un dato personal es preciso una vinculación entre información y un sujeto concreto – son precisos dos componentes que se sometan a tratamiento. (2005, pp. 104-105).

Igualmente, Nelson Remolina Angarita sostiene:

> El dato personal hace alusión a cualquier aspecto sobre una persona. La gama de información que se puede producir acerca de ella es diversa. Está relacionada con transacciones financieras, el consumo, la situación familiar, la solvencia económica, las creencias religiosas, la salud, los procesos y condenas criminales, la raza, la profesión u oficio, los títulos y grados económicos, el comportamiento sexual, el salario, las ideas políticas, los bienes, la familia o los datos de contacto (teléfono, dirección física o electrónica, etc. (2013, p. 133).

El GT 29 señala:

> Desde el punto de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas» (...) Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de esta. Por supuesto esto incluye la información personal considerada «datos sensibles» (...) pero también otras categorías más generales de información (...) Desde el punto de vista del formato o el soporte en que la información está contenida, el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo. Desde este punto de vista, el concepto incluye la información conservada en papel, así como la información almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video, por ejemplo. Se trata de una consecuencia lógica de la inclusión en su ámbito de aplicación del tratamiento automático de datos personales. En particular, los datos que consisten en sonidos e imágenes están calificados como datos personales desde este punto de vista, en la medida en que pueden contener información sobre una persona. (2007, pp. 6-7).

Lo importante, entonces, para el objeto del presente escrito, es que un dato personal no necesariamente hace referencia al nombre, apellido o identificación de alguien, pues, como señala el literal c) del artículo 3 de la Ley 1581 de 2012, es dato personal cualquier tipo de información asociada o que se pueda asociar a una o varias personas naturales determinadas o determinables. Este concepto comprende un sinnúmero de hechos, objetos y manifestaciones provenientes de una persona, como pueden ser sus comentarios, fotos, videos, preferencias, gustos, orientación sexual, ideología política, convicción religiosa, fisiología; estado de salud física, psicológica y social; situación económica y cultura, etc. Por lo tanto, existe una amplia gama de información considerada dato personal, que le corresponde al responsable del tratamiento determinar si esta se encuentra vinculada o podría vincularse a un sujeto físico identificado o identificable. En todo caso, si esa información no identifica, ni directa, ni indirectamente, al individuo, como sería

el caso de datos de carácter estadístico, no podemos hablar de dato personal. Un análisis similar puede aplicarse a los datos anónimos. Esto último resulta de la mayor importancia porque muchas empresas tratan información que no está sujeta al ámbito de aplicación de la Ley 1581 de 2012, lo cual no significa que no se encuentre sujeta a los principios rectores en materia de protección de datos personales, en especial, el principio de veracidad.

En ese marco es evidente, además, que todo dato personal es información, pero no toda información es un dato personal, pues lo importante en sí es que esta esté asociada directamente a un individuo o "si (...) se utiliza para determinar o influir en la manera en que se la trata o se la evalúa" (GT 29, 2005a, p. 8). En palabras más sencillas, lo que le da a una información la categoría de dato personal es, justamente, que verse sobre una persona física, es decir, que se refiera a ella, se reitera, directamente o indirectamente; este sería el caso, de cuando la información se refiere no tanto al aspecto físico del individuo sino a determinados objetos, procesos o hechos que le incumben como persona, verbigracia, el valor de su vivienda o el cuaderno de revisiones de su automóvil (GT 29, 2007, p. 10). Este es un elemento muy importante que se debe tener en cuenta en el momento en que una entidad recolecta cierta información que, a primera vista, no identifica al titular, y sin embargo, como dijo la Corte Constitucional, en Sentencia T-729 de 2002, citada en la Sentencia C-748 de 2011, "permite identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos", incluyendo dentro de este contexto todo tipo de afirmaciones subjetivas sobre el individuo. Ejemplos sobre ello hay muchos, pero, sin duda, el historial (*scoring)* financiero, que mide la probabilidad de que una persona incumpla una obligación crediticia a futuro y, que al mismo tiempo, permite ilustrar al analista de crédito sobre si el solicitante es buen o mal pagador, es una buena referencia sobre el tratamiento de afirmaciones subjetivas. En todo caso, "para que esas informaciones se consideren «datos personales», no es necesario que sean verídicas o estén probadas" (GT 29, 2007, p. 7). De igual manera, en muchas ocasiones, esa relación entre una persona y una información puede establecerse fácilmente. Al respecto, se dice en el Informe No. 136 del GT 29: "los datos incluidos en el fichero personal de una persona guardado en el departamento de personal de su empresa están claramente relacionados con su situación como empleado de dicha empresa" (2007, p. 10). Sin embargo, en ciertas ocasiones, no siempre resulta tan evidente; tal sería el caso, la dirección IP dinámica, pues bajo determinadas circunstancias esta información también se puede vincular a una persona.

Teniendo en cuenta que es dato personal toda aquella información que versa sobre una persona física, con independencia de si esta hace relación a su apariencia, comportamiento, cualidades, situación socioeconómica, habilidades, objetos o situaciones fácticas, se pasa a definir el concepto de *dato de localización*, ya que como se dejó planteado al inicio del presente capítulo, por regla general la posición geográfica

de un individuo es información de carácter personal, pues esta permite vincular fácil y rápidamente a una persona. Asimismo, este dato sirve como *identificador* para otro tipo de información dentro del mismo perímetro geográfico donde se moviliza el titular, incluso revela datos sensibles (por ejemplo del siguiente dato: la persona transita en un lugar que, a su vez, corresponde a la ubicación de la sede de un partido político; por tanto, se puede inferir, en mayor o menor medida, que ese individuo es miembro de esa organización política, lo que convierte ese tratamiento en sensible). Su absoluta precisión depende, obviamente, de las circunstancias concretas del caso y, en particular, de su combinación con información auxiliar, si esa persona ha votado por algún miembro de esa filiación. El resultado de este análisis permite evaluar el ámbito de aplicación de la Ley 1581 de 2012 sobre el tratamiento de los datos relacionados con la ubicación de un titular, por parte de una entidad pública o privada y, en especial: (i) informarle de manera clara y precisa sobre las finalidades del tratamiento; y, (ii) el tiempo de conservación de la información en sus sistemas operativos, así como la prohibición de usarla para otras finalidades no autorizadas por el individuo. Esto también significa que los proveedores de redes sociales deben guardar la confidencialidad sobre los otros tipos de datos detectados al momento en que conocen la posición geográfica del usuario.

1. Concepto de dato de localización

Como se ha visto a lo largo de este documento, un dato personal es aquella información relativa a un sujeto físico determinado o determinable, en particular, la relacionada con su paradero, ya sea directamente (localización de la propia persona) o indirectamente, como sería la localización del vehículo utilizado por él o de un producto o bien que se encuentre a su cargo (GT 29, 2005b). Sobre este último aspecto, la Agencia Española de Protección de Datos (AEPD), en Resolución No. 01208/2014 precisó lo siguiente:

> Como se refleja en el Informe Jurídico de esta Agencia arriba transcrito *estamos_ante un tratamiento automatizado de datos de carácter personal porque es posible, sin un esfuerzo desproporcionado, asociar la posición de los vehículos policiales, su localización, con los miembros de la policía que estén haciendo uso de tales vehículos, su identidad* [cursivas añadidas]. Los dispositivos instalados en los coches policiales emiten señales que controlan la hora de puesta en marcha y parada, recorrido efectuado, paradas intermedias, lugares exactos de situación y, en definitiva, su localización efectiva, obteniendo así datos del lugar en que se encuentra cada una de las personas por medio de los dispositivos instalados.

Del anterior panorama se desprende que de un objeto físico, en ese caso, un vehículo automotor, se puede detectar, entre otro tipo de información, el grado de impericia de su conductor y la posición geográfica de un individuo. Entonces, el criterio clave para el sentido y alcance del concepto de dato de localización es, como ya se analizó en párrafos anteriores y de

manera puntual en Sentencia T-729 de 2002 de la Corte Constitucional, "que el lugar de ubicación de una persona también puede ser identificado, en mayor o menor medida, gracias a la visión de conjunto que se logre con otros datos", entre ellos,

> datos procedentes de diversos sensores que van más allá de los datos de localización en sentido estricto, como los datos relativos al periodo de tiempo durante el cual se emplea una máquina o vehículo, el número de kilómetros recorridos o la velocidad a la que se ha desplazado el vehículo. (GT 29, 2005b, p. 11).

Ese aspecto permite, entre otros usos, que las empresas que ofrecen servicios de localización se valgan de datos adicionales para detectar dónde se encuentra geográficamente un usuario.

Teniendo en cuenta lo anterior, y siguiendo la misma línea de razonamiento, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002,[4] define al dato de localización como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público" (literal c) del artículo 2). A la vista del concepto establecido en la directriz europea, un dato de localización puede

> referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, 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. (Considerando No. 14).

Eso supone que la localización de una persona es capturada en frentes tridimensionales.

Lo anterior constituye una orientación suficiente para entender las diferentes técnicas de localización o, como va a ser mencionado en el siguiente capítulo, las infraestructuras destinadas a prestar servicios de geolocalización, tales como GPS, estaciones de base GSM y wifi, que son utilizados por los proveedores de plataformas de redes sociales con la finalidad, entre otras, de marcar la ubicación de un usuario en una foto (Instagram, 2013).

II. LOCALIZACIÓN EN LAS PLATAFORMAS DE COMUNICACIÓN EN LÍNEA O SERVICIOS DE REDES SOCIALES

En esta sección se explica en qué consisten los conceptos de localización (geolocalización) y georreferenciación, y su funcionamiento en las redes sociales. Para muchas personas son extraños estos dos conceptos, puesto que Fa-

4. 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).

cebook, Twitter, entre otras, inadvertidamente los utilizan o habilitan en sus equipos móviles; sin embargo, a veces la gente se pregunta por qué estas redes le ofrecen determinados servicios o le sugieren determinados productos de acuerdo con la ciudad en la que se encuentra localizada.

A. Concepto de sistemas de localización

La localización se define como "un concepto que hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (x), longitud (y) y altura (z)" (Beltrán, 2011, p. 25). Así mismo, el *Diccionario Oxford* define geolocalización como "el proceso o técnica que identifica la posición geográfica de una persona o un dispositivo por medios digitales e información procesada vía internet".[5]

De acuerdo con lo anterior, y debido a que en el *Diccionario de la lengua española* no existe una definición de *geolocalización*, el término adecuado es *localización*, que sí aparece allí con dos acepciones pertinentes para este estudio: "2. Averiguar el lugar en que se halla alguien o algo. 3. Determinar o señalar el emplazamiento que debe tener alguien o algo" (Real Academia Española, 2015). Por lo tanto, como fue abordado en el anterior capítulo, la localización consiste en determinar la posición geográfica de una persona dentro de un espacio, mediante las coordenadas latitud (x), longitud (y) y altura (z) vía Internet o con otros dispositivos digitales.

Por otro lado, la georreferenciación es el "uso de coordenadas de mapa para asignar una ubicación espacial a entidades cartográficas" (ArcGIS, s.f., párr. 1). En términos más sencillos, la georreferenciación busca establecer la ubicación de determinado punto dentro de un sistema de coordenadas de una foto aérea o satelital, con el fin de convertir las coordenadas de la imagen en coordenadas de mapa. Por lo tanto, se puede deducir que la localización y la georreferenciación buscan, en el caso que nos ocupa, determinar la ubicación de un individuo.

Los sistemas de localización permiten identificar la ubicación física de un usuario final a través de la Internet (King, 2010). El método más sofisticado y comúnmente utilizado es la dirección IP del usuario final. Este método funciona de la siguiente manera: (i) cuando el usuario escribe una URL (localizador de recursos uniforme) en su navegador (entre ellos, Google, Mozilla o Big), o hace clic en un hipervínculo, dicha solicitud de acceso se envía al servidor donde opera el sitio Web; (ii) cuando ese servidor recibe la solicitud de acceso, este envía una solicitud de ubicación de la dirección IP del usuario al proveedor de servicios de geolocalización; (iii) el proveedor de servicios de geolocalización, con base en la información de

5. "The process or technique of identifying the geographical location of a person or device by means of digital information processed via the Internet."

las direcciones IP en uso, recopiladas por él en su base de datos, le suministra al servidor del sitio Web una pista de dónde se encuentra la ubicación del usuario final; y, (iv) con esa información, el servidor Web proporciona el acceso al usuario final (Svantesson, 2004, pp. 101,109-110).

La mayoría de expertos consideran que la localización por medio de un sistema basado en las direcciones IP es exacta, dado que su porcentaje de precisión se encuentra en un rango del 85 % al 98 % (Market Wired, 2009). Sin embargo, la precisión y exactitud en la ubicación mediante esta tecnología dependerá de la calidad de los datos que utilice el proveedor de la localización, su funcionamiento, y la arquitectura de Internet que prevalezca.

Existen otras tecnologías utilizadas para la localización del usuario final, como solicitar al navegador web la configuración de la zona horaria y el idioma para determinar la ubicación física (*geolocation and federalism on the internet: cutting internet gambling's gordian knot*).

Actualmente, muchas empresas y proveedores de redes sociales utilizan herramientas basadas en localización, para ofrecer sus productos o servicios, o para restringir el acceso a ciertos contenidos que no se encuentran disponibles en determinada ubicación. A continuación se mencionan algunos de los servicios de localización referidos por Beltrán López (2012, p. 22):

- Los geoportales con los que se puede generar y obtener información geográfica, con herramientas como Google Maps, Google Earth, Openstreetmap, Ikimap, etc.
- La geolocalización social, con la cual es posible compartir información, con herramientas como Foursquare, Gowalla, Twitter, Facebook y Google +.
- La geolocalización aumentada, útil para innovar, con herramientas como Layar, Junaio y Wikitude.
- El geomarketing y el geocommerce, como forma de promocionar y vender.
- El geoposicionamiento web, con herramientas como Google Places.

Es así como los dispositivos móviles y las herramientas de localización,

> al combinarse con la posición del usuario que está en movimiento, pueden obtener información única para cada persona, basada en la posición en que se encuentra, de ahí el interés que suscita en el mundo de la publicidad. Así, algunas de las aplicaciones y sitios web para móviles aprovechan esta funcionalidad. (Arroyo Vásquez, 2011, p. 43).

En este capítulo se ofreció una explicación general del funcionamiento de los sistemas de localización y cómo diferentes proveedores los utilizan para prestar sus servicios. A continuación se explican con más detalle estas tecnologías de localización.

1 Sistemas de localización

La gran cantidad de recursos desplegados por las empresas para conocer los gustos, prefe-

rencias y sitios donde se encuentran ubicados los usuarios de sus servicios permitió que en los últimos diez años evolucionaran sustancialmente los sistemas de localización, al punto que actualmente identificas la geoposición, latitud, longitud y altitud, lo que facilita establecer la ubicación de una persona en determinado espacio de tiempo (Cheung, 2014).

Ahora, gracias a la introducción de la localización basada en servicios (*Location Based Services* -LBS), es posible identificar en tiempo real la posición de un usuario (Hildebrandt, 2012), por medio de los sistemas que se explican a continuación. Estos sistemas pueden determinar la ubicación de una persona, ya sea por GPS, la identificación de la posición del dispositivo celular o mediante la red wifi o IP del usuario. Adicionalmente, existen otro tipo de herramientas que utilizan más de un sistema a la vez para identificar la localización, como es el asistido por GPS (A-GPS) (Cheung, 2014).

En primer lugar, los GPS[6] son sistemas que utilizan una constelación de 31 satélites para proporcionar la posición precisa de una persona, en tiempo real, mediante la trilateración, es decir, la longitud, latitud y altitud (Fischetti, 2008).

Seguidamente, la identificación por medio del dispositivo celular se determina mediante la triangulación del lugar en que se encuentra ubicado un equipo en su posición actual. Uno de los métodos más populares utiliza la estación en la que se encuentra conectado el dispositivo para determinar la posición del equipo (Cell of Origin);[7] funciona mediante la identificación de la estación base (*cell id*), estimando la dirección de la señal proveniente del dispositivo (Schmidt-Dannert, s.f.).

Del mismo modo, la técnica de diferencia observada en el tiempo de llegada (*Enhanced-Observed Timed Difference* –E-OTD), utiliza dos o más estaciones base para calcular la localización del dispositivo móvil (Marker, s.f.).

También existen otros métodos que utilizan los mismos principios, pero calculan el tiempo de llegada, el ángulo y la diferencia observada entre el tiempo de llegada de la señal, para determinar la posición (Marker, s.f.).

Un tercer tipo de sistemas, basados en localización con GPS asistido (A-GPS), funcionan de la siguiente manera: una vez la persona se conecta con la estación base, esta información se envía a un servidor externo, la ID de la antena, y el teléfono obtiene como respuesta los satélites que tiene encima y su posición (están almacenados en el servidor externo). (Tróito.com, 2013).

En cuarto lugar, la identificación de la posición por medio de las redes de wifi, es un sistema basado en localización que permite identificar la posición de un usuario determinando la ubicación del punto de acceso al que se encuentra conectado. Para establecer la localización,

6. La precisión de este sistema es de 4 a 15 metros.

7. La precisión es de 50 metros en una ubicación densamente poblada.

este método establece cuál es la dirección MAC (*Media Access Control*) de cada uno de los puntos wifi a los que el dispositivo se conecta; también pueden existir herramientas que permiten determinar dónde se encuentra el equipo, calculando la fuerza de la señal con la que se contacta a la red (GT 29, 2011).

Declan McCullagh (2011), en su escrito titulado "Google's Web mapping can track your phone", señala que casi nadie se había dado cuenta que Google identificó la localización de varios dispositivos móviles conectados a redes wifi, estableciendo la dirección MAC de cada uno de ellos, y publicado dicha ubicación. Esto, dice, pudo ser realizado porque los dispositivos que se conectan a redes wifi cuentan con su propia dirección MAC, la cual fue recolectada y publicada por Google.

Por último, existen sistemas para identificar los equipos móviles, que vienen instalados dentro de los equipos de fábrica. Uno de los más famosos es Find My iPhone, que se encuentra preconfigurado en todos los dispositivos Apple. En Corea se encontró culpable a dicha empresa por instalar este tipo de sistema sin que los usuarios permitieran su funcionamiento (Cheung, 2014).

B. Localización en las plataformas de comunicación en línea o servicios de redes sociales

En los últimos años el uso de las redes sociales ha crecido exponencialmente, como se evidencia en el ranking de los 500 sitios de Alexa más visitados en la web, donde aparece Facebook en segundo lugar (Alexa. An amazon.com company, s.f.). Allí mismo, el ranking de servicios de comunicación en línea para Colombia la lideran YouTube, Google.com, Facebook, Google.com.co, y así sucesivamente. Es importante mencionar que dichas plataformas web deben su éxito a que permiten a sus usuarios mantenerse en contacto.

Las redes sociales son plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes (GT 29, 2009). En otras palabras, una red social se define como la representación digital de los usuarios, sus amistades, fotos, artículos, sitios visitados, etc. Es por esta razón, que parte de su modelo de negocio es identificar la ubicación del usuario o personas en común, con el fin de sugerir grupos de contactos precisos con base en intereses comunes, actividades y productos o servicios dentro de su localización.

Al respecto es preciso entender que existen dos tipos de redes: las que funcionan dentro de una arquitectura cliente-servidor y las funcionan mediante la arquitectura peer-to-peer. En las primeras la información se encuentra centralizada en un servidor, y es allí donde funciona la plataforma; en las segundas la información se encuentra distribuida entre los diferentes usuarios de la red, es decir, no se encuentra centralizada (De Luz, 2010).

La mayoría de plataformas se encuentran centralizadas (Facebook o Twitter, entre otras), lo

que permite que toda la información funciona en el esquema cliente-servidor, ya que todo el contenido —imágenes, noticias o sitios visitados— se encuentra almacenado en los servidores de las compañías. Como consecuencia, estos proveedores incorporaron nuevas herramientas, como la ubicación de sus usuarios.

Se puede concluir que el modelo de negocios de este tipo de servicios funciona en el "intercambio o consumo de información personal", dado que las redes sociales

> ofrecen al usuario servicios aparentemente gratuitos pero cuya contraprestación no es otra que acceder a datos personales del usuario, –como su perfil de navegación, su lista de amigos, o el contenido de los mensajes que escribe o recibe–, obtener información directamente requerida al usuario con finalidades como la elaboración de perfiles de consumo o personalidad, o remitirle determinada información o publicidad. En estos casos la información legal y las políticas de privacidad suelen mostrar que no se trata de un "servicio gratuito", ya que el usuario "abonará" el servicio con su información personal. (AEPD, 2009, p. 6).

En esa misma línea, dicha Agencia en su *Guía de recomendaciones de Internet,* señaló:

> A través de las redes sociales es posible compartir información personal y contactar con otros usuarios de la Red. En la práctica el funcionamiento de estos servicios comporta que cada usuario ponga a disposición de otros muchos, con los que no tiene por qué tener una relación de confianza, multitud de información personal. Generalmente en las redes sociales se denomina 'amigo' a alguien que simplemente nos ha hecho llegar una tarjeta de presentación o que conforme a las reglas del portal 'es amigo de un amigo'. El empleo de expresiones del tipo 'amigo', 'tu muro', o 'tu álbum de fotografías' ofrecen una falsa imagen de privacidad para lo que, si no se conoce el funcionamiento de la red social acaba siendo público y disponible para cualquier persona. De hecho, si se utilizan las configuraciones por defecto, lo habitual es que la información sea completamente disponible para cualquier tercero, incluidos los buscadores. (AEPD, 2009, p. 40).

Ahora bien, como se discutió previamente, existen redes sociales que se les conoce por su nombre en inglés como Location Based Social Networks (LBSN), toda vez que permiten compartir la ubicación de los usuarios utilizando algún sistema basado en localización, ya sean equipos móviles o computadores de escritorio. Este tipo de portales les ofrece a sus usuarios dos formas para compartir su posición:

La primera mediante el *geotagging,* en el que los videos, fotos, blog post o tweets son convertidos en información geográfica, y el usuario identifica dónde se encuentra ubicado en ese instante. Flickr (http://flickr.com) permite conocer la localización de imagen a través de los datos EXIF o cuando sus usuarios comparten las coordenadas en un mapa habilitado para dicho propósito.

La segunda, cuando los usuarios comparten en su perfil su ubicación actual. En Foursquare (http://foursquare.com) las personas señalan que se encuentran en determinado restaurante y publican de esa forma su localización. Esta forma de compartir la posición se conoce en inglés como geosocial networking, que incentiva a compartir la información por medio de juegos o aplicaciones gratuitas (Gordon y De Souza, 2011, pp. 362-363).

Es el caso de Facebook, red que automáticamente permite conocer la ciudad del usuario, y de esa manera actualiza la configuración y la localización de sitios como restaurantes o tiendas. Igualmente, en Twitter los usuarios pueden compartir información de localización en sus actualizaciones, gracias a las opciones en la configuración (Twitter, s.f.).

Por estas razones, las autoridades de protección de datos a nivel mundial y los académicos han tomado más en serio el tratamiento que están dando a los datos personales en las redes sociales. Más aún, cuando son recolectados, tratados y compartidos por estos servicios web, como sucede en Foursquare o Messenger de Facebook,[8] sin que exista una autorización o, en algunos casos, sin que muchos de los usuarios conozcan la finalidad del tratamiento o los derechos que les asisten frente a estos servicios.

Al mismo tiempo se han identificado tres riesgos a la privacidad de los sistemas de localización, que deberían ser tenidos en cuenta tanto por las redes sociales como por los usuarios: (i) riesgo de privacidad de localización, que quiere decir que cualquier persona puede conocer dónde se encuentra determinada persona en cierto momento; (ii) riesgo de ausencia de privacidad, que implica poder conocer que una persona no se encuentra en determinado sitio, por ejemplo, en el trabajo; y, (iii) riesgo de co-localización de privacidad, en el cual una persona se puede localizar por medio de la identificación de otros usuarios con algún tipo de vínculo dentro del portal (Gordon y De Souza, 2011, pp. 362-363).

En la misma línea, la AEPD señaló los riesgos que presenta la Internet para los datos personales y la identificación de los usuarios:

> Los servicios de geolocalización pueden tener un gran impacto en la privacidad de los usuarios, debido en gran parte a que la tecnología de dispositivos móviles inteligentes (Smartphones) permite la monitorización constante de los datos de localización. Estos dispositivos están íntimamente ligados a una persona concreta y, normalmente, existe una identificabilidad directa e indirecta del usuario. (2014a, párr. 32).

Así pues,

> Esta tecnología, que puede llegar a revelar detalles sobre la vida privada de su propietario, permite a los proveedores de servi-

8. Ver Khanna (2015).

> cios de geolocalización una visión personal de los hábitos y los patrones del propietario del dispositivo y crear perfiles exhaustivos. Uno de los riesgos de la utilización de esta tecnología es que los usuarios no son conscientes de que pueden estar transmitiendo su ubicación, ni a quién. (AEPD, 2014a, párr. 33).

En ese orden de ideas, los datos tratados por las redes que utilizan sistemas basados en localización deben ser considerados como datos privados, y por esta razón, por lo menos en Colombia, se deberá remitir a la definición que trae la Ley 1266 de 2008, que señala: "Dato privado. Es el dato que por su naturaleza íntima o reservada solo es relevante para el titular" (literal h), del artículo 3 de la Ley 1266 de 2008). En consecuencia, se deberían plantear dos escenarios en los que estos datos son tratados: el primero, cuando las redes sociales adoptan sistemas basados en localización, con el propósito de enriquecer la experiencia del usuario en la interfaz; el segundo, cuando los usuarios comparten su ubicación a sus contactos dentro de la red social.

En ambos casos, el usuario deberá ser quien autorice el funcionamiento de los sistemas basados en localización, como se menciona más adelante dentro de las obligaciones que deben implementar estos portales cuando decidan prestar servicios que incorporan la ubicación de los usuarios.

Las siguientes herramientas deberían ser modificadas por las redes sociales, de acuerdo con las observaciones que se presentan más adelante: (i) Facebook: la opción de localizar a los usuarios y sus acciones en el muro;[9] (ii) Twitter: los tweets que lanza tienen la opción de seleccionar la localización;[10] (iii) LinkedIn: la opción "Ubicaciones principales en tu red" en el apartado de estadísticas, localización y redes sociales;[11] (iv) Foursquare: opción de los usuarios de hacer pública su localización; y (iv) Instagram: posibilidad de identificar la ubicación donde fue tomada la foto, en función de las personas, los lugares y las etiquetas[12] (Mendoza Enríquez, 2014). Lo anterior fue reiterado por el GT 29 en su informe sobre la incidencia en la privacidad de los servicios de geolocalización en dispositivos móviles inteligentes, de 2011.

Finalmente, se encuentra que los sistemas basados en localización pueden generar un alto impacto en la protección de los datos de las personas. La mayoría de los casos se genera por la falta del consentimiento. Pero también porque los responsables del tratamiento, en particular los proveedores de los servicios de redes sociales, no están informando de una manera clara las finalidades por las cuales están recolectando ese tipo de información.

9. www.facebook.com/myfriendmap
10. http://tweepsmap.com/Geolocalización
11. http://www.linkedin.com/
12. https://www.instagram.com/developer/endpoints/locations/

No obstante lo anterior, en el siguiente capítulo se propone una serie de prácticas que pueden ser incorporadas por estas redes sociales, con el fin de realizar un tratamiento legal de los datos personales de localización, en cumplimiento de lo dispuesto en las normas que regulan esta materia.

1. Obligaciones de los proveedores de plataformas de comunicación en línea o servicios de redes sociales

La gran preocupación que se pone de presente en este punto, como se ha reiterado a lo largo de esta investigación, es la omisión de la industria en línea, especialmente de los proveedores de servicios de redes sociales, de requerir el consentimiento de sus usuarios para tratar la información relacionada con su ubicación física. En la mayoría de los casos, se abstienen de informarle al usuario el cómo, ante quién, desde cuándo, por cuánto tiempo y para qué su dato será utilizado (CConst., T-593/2003, A. Tafur).

Pero, más grave aún: la combinación simultánea de herramientas de sistemas de localización —estaciones de base, puntos de acceso wifi y GSP—, con el objetivo, entre otros, de tener un monitoreo continuo y en tiempo real de los movimientos de una persona, genera un efecto nocivo en la intimidad del individuo. Esta circunstancia se agrava significativamente debido a que "la tecnología en línea de hoy avanza a un ritmo más rápido que las leyes de privacidad de la sociedad" (Jaeger, 2014, p. 394).

Las anteriores circunstancias hacen necesario que los proveedores de plataformas de comunicación en línea se adhieran a códigos de buenas prácticas, que permitan a los cibernautas conocer qué empresas de la Web han adoptado medidas reales y eficaces de protección de datos. Esta decisión debe ser, además, divulgada al público. Esto podría ser mediante la publicación de una lista de entidades autorreguladas en la página web de las autoridades de protección de datos, sin que estas pierdan su competencia de vigilancia y control, y al mismo tiempo promover la adopción de guías de estándares de privacidad dentro de la industria del Internet.

Son elementos de un código de buena conducta: (i) el compromiso de requerir el consentimiento de los usuarios, de manera previa a que sus sistemas de localización identifiquen sus posiciones geográficas. En la práctica ello se traduce, por citar algunas razones, en la prohibición de recolectar datos en secreto; y (ii) la obligación de informarle al usuario las finalidades del tratamiento y, en concreto, en qué momento y por cuánto tiempo esos sistemas estarían autorizados para conocer su ubicación, a saber: por una operación específica o de manera permanente, sin que sea admisible, en consecuencia, cláusulas vagas e imprecisas. Eso incluye, obviamente, indicar si ese dato será compartido con terceros y qué tipo de terceros. Al respecto CTIA The Wireless Association (2010) señala:

- Primero, los proveedores de servicios de localización deben informar a los usuarios

acerca de cómo su información de localización será usada, divulgada y protegida, de tal manera que puedan decidir si autorizan o no el uso de sistemas basados en localización o si autorizan su divulgación.

- Segundo, una vez los usuarios han escogido usar un sistema basado en localización o han autorizado la divulgación de su información de ubicación, él o ella deberán tener opciones sobre si esa información será compartida a terceras partes y deberán tener la capacidad para revocar cualquier autorización. (p. 1).

En línea con lo anterior, los proveedores de servicios de redes sociales deben: (i) ser transparentes[13] en relación con sus políticas de privacidad. Cabe precisar que estas reglas deben ser claras, concisas y un fiel reflejo de cómo están utilizando los datos de localización; (ii) adoptar herramientas para que el sujeto concernido pueda en cualquier momento revocar su autorización; (iii) facilitar al titular el acceso a la información recolectada a través de sistemas basados en localización; (iv) implementar mecanismos de «diseño por privacidad» o «privacy by design» para evaluar el impacto, valga la redundancia, en la privacidad al momento de desarrollar productos o servicios basados en la localización de sus clientes; y, finalmente, (v) crear conciencia en los cibernautas sobre los riesgos potenciales al momento en que acceden a páginas web o descargan aplicaciones que carezcan de sistemas de seguridad robustos que permitan, entre otros incidentes, el acceso no autorizado a sus datos personales, o simplemente explicarles cómo pueden desactivar la opción "compartir su ubicación" o impedir que los rastreen. Una forma podría ser mediante la publicación de videos que les enseñen cómo activar las funciones de cifrado en los *routers* inalámbricos para proteger sus redes domésticas (Federal Communications Commission, 2012, p. 6)

La adopción de estándares de buenas conductas refleja un equilibrio entre el respeto y protección de los derechos fundamentales al *habeas data* e intimidad de los titulares de la información y el poder informativo de los proveedores de servicios de redes sociales.

III. CONCLUSIONES

Hoy en día la industria del Internet recolecta grandes cantidades de información de sus clientes mientras estos acceden a su perfil de red social, leen un periódico en línea (*online)* o simplemente buscan información en un motor de búsqueda. Esto ha permitido, en gran medida, que los ciudadanos cedan el control de sus datos a las grandes compañías de Silicon Valley, como son Facebook o Google.

Aunado a lo anterior, los datos personales son, en la actualidad, uno de los principales activos

13. Ley 1581 de 2012, artículo 4, literal e. "Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan;"

de las organizaciones. De hecho, las compañías están desarrollando sus productos o servicios basados en el comportamiento en línea de la persona (esto en virtud del llamado Online Behavioural Advertising). Entre sus insumos se encuentra el dato de localización, ya que, como pudo apreciarse en párrafos precedentes, les permite ofrecer con mayor precisión y en tiempo real bienes, productos y servicios de acuerdo con una específica ubicación geográfica.

Amén de lo anterior, es evidente que las redes sociales usan sistemas de localización (GPS, redes wifi, torres de telefonía móvil o iBeacons) para detectar la ubicación de sus usuarios en un determinado espacio y tiempo. El servicio de Facebook "Amigos Cerca" es un claro ejemplo de ello. Se trata, por tanto, de herramientas que están al servicio de los proveedores de las plataformas de comunicación en línea, sin que, se reitera, se le haya informado previamente a la persona sobre este tipo de tratamiento. Esto es una conducta claramente contraria a las normas sobre protección de datos.

Es necesario, por tanto, que los proveedores de servicios de redes sociales adopten medidas y procedimientos internos en función de la naturaleza del dato de localización o se adhieran a estándares de la industria, también conocidos como códigos de buenas prácticas, tendientes a garantizar en la práctica la observancia de los principios rectores para el tratamiento de datos personales (tal como restringir la obtención de datos personales al mínimo necesario) y que, al tiempo, minimicen los riesgos jurídicos, económicos y de prestigio que podrían derivarse de una práctica precaria de protección de datos (GT 29, 2010, p. 6). Esto les permitiría conseguir una ventaja competitiva frente a su competencia y, de paso, para el caso colombiano, demostrarle a la Superintendencia de Industria y Comercio que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.[14]

Referencias

1. Agencia Española de Protección de Datos [AEPD]. (2009). *Recomendaciones a usuarios de internet.* Recuperado el 15 de febrero de 2016, de agdp: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf

2. Agencia Española de Protección de Datos. (2014a). *Servicios de Internet y riesgos para sus datos personales*. Recuperado el 21 de febrero de 2016, de agpd: https://www.agpd.es/portalwebAGPD/jornadas/dia_internet_2014/servicios_y_riesgos-ides-idphp.php#seccion6

3. Agencia Española de Protección de Datos. (2014b). Resolución R/01208/2014.

14. Véase Superintendencia de Industria y Comercio (2015).

4. Alexa. An amazon.com company. (s. f.). *The top 500 sites on the web*. Recuperado el 15 de febrero de 2016, de Alexa: http://www.alexa.com/topsites

5. Apple, Inc. (17 de 09 de 2015). Acerca de la privacidad y Localización en iOS 8 y posteriores. Recuperado el 14 de febrero de 2016, de support.apple: https://support.apple.com/es-es/HT203033

6. ArcGIS. (s.f.). *Georreferenciación y sistemas de coordenadas*. Recuperado el 14 de febrero de 2016, de resources.arcgis: http://resources.arcgis.com/es/help/getting-started/articles/026n0000000s000000.htm

7. Arroyo Vásquez, N. (2011). *Informe APEI sobre movilidad*. Recuperado el 14 de febrero de 2016, de leprints: http://eprints.rclis.org/15898/1/informeapeimovilidad.pdf

8. Beltrán López, G. (26 de mayo de 2011). *Geolocalización y empresa*. En entrevista a Laura Mateo Catalán. Recuperado el 14 de 02 de 2016, de https://laurymat.wordpress.com/2011/05/26/geolocalizacion-y-empresa-entrevista-a-gerson-beltran-profesor-del-curso-de-community-manager-de-la-universidad-de-alicante/

9. Beltrán López, G. (2012). *Geolocalización y redes sociales. Un mundo social, local y móvil.* Madrid: Bubok.

10. Camperos Vivas, P. A. (s.f.). Geolocalización. Obtenido de http://pruebaotra12.blogspot.com.co/p/blog-page_13.html

11. P. A. Citron, D. (24 de diciembre de 2014). *BEWARE: The Dangers Of Location Data*. Obtenido de Forbes: https://www.forbes.com/sites/daniellecitron/2014/12/24/beware-the-dangers-of-location-data/#68749a0843cb

12. Clarke, R. (13 de diciembre de 2000). *Person-Location and Person-Tracking: Technologies, Risks and Policy Implications.* Recuperado el 18 de enero de 2016, de rogerclarke: http://www.rogerclarke.com/DV/PLT.html

13. Congreso de la República de Colombia. Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. Nº 48.587.

14. Corte Constitucional de Colombia. Sentencia T-729 de 2002 (M. P.: Eduardo Montealegre Lynett; septiembre 5 de 2002).

15. Corte Constitucional de Colombia. Sentencia T-593 de 2003 (M. P.: Álvaro Tafur Galvis; julio 17 de 2003).

16. Cottrill, C. D., & Thakuriah, P. (2014). Privacy in context: an evaluation of policy-based approaches to location privacy protection. *International Journal of Law and Information Technology, 22*(2), 178-207.

17. ctia Wireless Association. (2010). Best Practices and Guidelines for Location-Based Services. Obtenido de ctia.org: https://www.ctia.org/initiatives/voluntary-guideli-

nes/best-practices-and-guidelines-for-location-based-services.

18. Cheung, A. S. (2014). Location privacy: The callenges of movile service devices. *Computer Law & Security Review, 30*(1), 41-54.

19. De Luz, S. (11 de noviembre de 2010). *Privacidad y Seguridad en las Redes Sociales*. Obtenido de redeszone: https://www.redeszone.net/seguridad-informatica/redes-sociales/

20. Domínguez, M. (25 de marzo de 2014). Qué pasos tengo que hacer para que mi pág. tenga un mapa? *Pensamientis Universitarios* [blog]. Obtenido de http://ariipijamas.blogspot.com.co/2014/03/geolocalizacion.html

21. Gordon, E. & De Souza Silva, A. (2011). Net Locality: Why Location Matters in a Networked World. *Journal of Media Literacy Education*, 5(1), 362-363. Recuperado el 21 de 02 de 2016, de http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1121&context=jmle

22. Doty, N., Mulligan, D. K., & Wilde, E. (Febrero de 2010). *Privacy Issues Of The W3c Geolocation Api*. Obtenido de escholarship: http://escholarship.org/uc/item/0rp834wf

23. *El País*. (12 de marzo de 2010a). *Twitter geolocaliza los mensajes*. Recuperado el 12 de enero de 2014, de tecnología.elpais: http://tecnologia.elpais.com/tecnologia/2010/03/12/actualidad/1268388065_850215.html

24. *El País*. (29 de abril de 2010b). *Alemania denuncia que Street View almacena datos de las redes wi-fi de los particulares*. Recuperado el 6 de enero de 2016, de tecnología.elpais: http://tecnologia.elpais.com/tecnologia/2010/04/29/actualidad/1272531662_850215.html

25. Facebook. (s.f.). *Política de datos.* Recuperado el 14 de febrero de 2016, de https://www.facebook.com/about/privacy

26. Federal Communications Commission. (2012). *Location-based services an overview of opportunities and other considerations.* Obtenido de Benton Foundation: https://www.benton.org/node/124363

27. Fischetti, M. (1 de diciembre de 2008). Where on Earth You Are—Working Knowledge on Global Positioning System. *Scientific American*.

28. Gan, D., & Jenkins, L. R. (2015). Social Networking Privacy—Who's Stalking You? *Future Internet, 7*(1), 67-93.

29. *Google Europe Blog. (27 de abril de 2010). Data Collected by Google Cars*. Recuperado el 6 de enero de 2015, de googlepolicyeurope: http://googlepolicyeurope.blogspot.com.co/2010/04/data-collected-by-google-cars.html

30. Grupo de Trabajo del Artículo 29. (2005a). *Working document on data protection issues related to RFID technology.* Recuperado el 13 de febrero de 2016, de ec.europa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf

31. Grupo de Trabajo del Artículo 29. (25 de noviembre de 2005b). *Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido*. Recuperado el 14 de febrero de 2016, de ec.europa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_es.pdf

32. Grupo de Trabajo del Artículo 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales*. Recuperado el 13 de febrero de 2016, de ec.europa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

33. Grupo de Trabajo del Artículo 29. (2009). *Dictamen 5/2009 sobre las redes sociales en línea*. Recuperado el 15 de febrero de 2016, de ec.europa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf

34. Grupo de Trabajo del Artículo 29. (2010). *Dictamen 3/2010 sobre el principio de responsabilidaden línea*. Recuperado el 23 de febrero de 2016, de ec.europa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf

35. Grupo de Trabajo del Artículo 29. (2011). *Opinion 13/2011 on Geolocation services on smart mobile devices*. Recuperado el 12 de enero de 2016, de ec.europa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

36. Herrán Ortiz, A. I. (2002). *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales.* Madrid, España: Dykinson.

37. Hildebrandt, M. (2012). The Dawn of a Critical Transparency Right for the Profiling Era. *Digital Enlightenment Yearbook,* 41-56.

38. Instagram. (January 19, 2013). *Privacy Policy*. Recuperado el 16 de febrero de 2016, de help.instagram: https://help.instagram.com/155833707900388

39. *Information Systems Audit and Control Association [Isaca]*. (2011). *Geolocation: Risk, Issue and Strategies.* Rolling Meadows, Illinois: ISACA.

40. Jaeger, E. (2014). Facebook Messenger: Eroding User Privacy in Order to Collect, Analyze, and Sell Your Personal Information. *The John Marshall Journal of Information Technology & Privacy Law, 31*(3), 392-421.

41. Khanna, A. (August 11, 2015). Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger. *Technology Science*. 2015081101. August 11, 2015. https://techscience.org/a/2015081101

42. King, K. F. (2010). Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot. *The Columbia Science and Technology Law Review, 41*.

43. Lee, B. (14 de mayo de 2007). *Privacy and Awareness on Facebook.com*. Obtenido de semanticscholar: https://pdfs.semanticscholar.org/b0a9/39c346f944e4bd414f709d54e4cb88dd9b6d.pdf

44. Marker, G. (s. f.). *Localización de teléfonos celulares por GSM y GPS*. Recuperado el 16 de febrero de 2016, de informática-hoy: http://www.informatica-hoy.com.ar/soluciones-moviles/Localizacion-de-telefonos-celulares-por-GSM-y-GPS.php

45. Market Wired. (14 de abril de 2009). *PricewaterhouseCoopers (PwC) Completes Annual Audit of Quova IP Geolocation Data*. Recuperado el 21 de febrero de 2016, de marketwired: http://www.marketwired.com/press-release/pricewaterhousecoopers-pwc-completes-annual-audit-of-quova-ip-geolocation-data-1233911.htm

46. Mccullagh, D. (11 de junio de 2011). *Exclusive: Google's Web mapping can track your phone*. Recuperado el 16 de febrero de 2016, de c/net: http://www.cnet.com/news/exclusive-googles-web-mapping-can-track-your-phone/

47. Mendoza Enríquez, O. (5 de noviembre de 2014). *La geolocalización y la protección de datos personales datos personales.* Recuperado el 21 de febrero de 2016, de oiprodat.com: http://oiprodat.com/2014/11/05/la-geolocalizacion-y-la-proteccion-de-datos-personales/

48. Nolan, P., & Tobin, O. (2011). Geolocation services — where does the Article 29 Working Party stand? *Data Protection Ireland Journal, 4*(4).

49. Olenski, S. (17 de enero de 2013). *Is Location Based Advertising The Future Of Mobile Marketing And Mobile Advertising?* Obtenido de Forbes: http://www.forbes.com/sites/marketshare/%202013/01/17/is-location-based-advertising-the-future-of-mobile-marketing-and-mobile-advertising/

50. Oxford. (s.f.). Oxford Dictionaries. Recuperado el 21 de 02 de 2016, de http://www.oxforddictionaries.com/es/definicion/ingles_americano/geolocation

51. Oxford. (s. f.). *Oxford Dictionaries*. Recuperado el 21 de febrero de 2016, de oxforddictionaries: http://www.oxforddictionaries.com/es/definicion/ingles_americano/geolocation

52. Parlamento Europeo. 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 (Directiva sobre la privacidad y las comunicaciones electrónicas). Obtenido de ecx.europa: http://ec.europa.eu/justice/data-protection/law/files/recast_20091219_es.pdf

53. Payeras Capellá, M. M., Mut Puigserver, M., Paniza Fullana, A. e Isern Deyà, A. P. (2014). Privacidad en servicios turísticos basados en geolocalización. *Revista de Derecho, Empresa y Sociedad,* (5), 78-93.

54. Real Academia Española. (s. f.). *Diccionario de la lengua española*. Recuperado el 12 de 02 de 2016, de http://dle.rae.es

55. Remolina Angarita, N. (2013a). *Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012*. Bogotá: Legis Editores S.A.

56. Schmidt-Dannert, A. (s. f.). *Positioning Technologies and Mechanisms for mobile Devices*. Recuperado el 16 de 02 de 2016, de https://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS10/snet-project/positioning-technologies_schmidt-dannert.pdf

57. Superintendencia de Industria y Comercio. (2015). Guía para la implementación del principio de responsabilidad demostrada (Accountability).

58. Svantesson, D. J. (Fall 2004). Geo-location technologies and other means of placing borders on the 'borderless' internet. *Journal of Computer & Information Law, 23*, 100-139. Recuperado el 21 de febrero de 2016 de: http://repository.jmls.edu/cgi/viewcontent.cgi?article=1051&context=jitpl

59. Tróito.com. (marzo de 2013). *¿Qué es el ¨A-GPS¨ que incorpora mi smartphone?* Recuperado el 16 de febrero de 2016, de troito.com: http://www.troito.com/2013/03/que-es-el-gps-que-incorpora-mi.html

60. Twitter. (s.f.). FAQs about adding location to your Tweets. Recuperado el 21 de 02 de 2016, de https://support.twitter.com/articles/78525?lang=en

61. Vesalga, A. D. (2013). Location, Location, Location: Updating the Electronic Communications Privacy Act to Protect Geolocational Data. *Golden Gate University Law Review, 43*(3), 458-483. Recuperado el 20 de 01 de 2016, de http://digitalcommons.law.ggu.edu/ggulrev/vol43/iss3/5

62. Vilasau Solana, M. (2005). Derecho de intimidad y protección de datos personales. En M. Pequera Poch, *Derecho y nuevas tecnologías* (pp. 104-105). Barcelona: Editorial UOC.