PRIVACIDAD EN SERVICIOS TURISTICOS BASADOS EN GEOLOCALIZACIÓN

MARIA MAGDALENA PAYERAS CAPELLÀ
Doctora en Ingeniería

ANTONIA PANIZA FULLANA
Doctora en Derecho

MACIÀ MUT PUIGSERVER
Doctora en Ingeniería

ANDREU PERE ISERN DEYÀ
Doctor en Ingeniería

Fecha de recepción: 14 de diciembre de 2014
Fecha de aceptación: 29 de diciembre de 2014

RESUMEN: *Los servicios basados en geolocalización (Location-BasedServices, LBS) son servicios que ofrecen a los usuarios información acerca del entorno en el que están situados, como restaurantes cercanos, cines, puntos de interés turístico, etc. Existen multitud de aplicaciones relacionadas con el comercio electrónico que incorporan servicios LBS. También se han publicado recientemente numerosas aplicaciones relacionadas con el sector turístico que utilizan servicios LBS: turistas y ciudadanos demandan información relacionada con su posición en sus viajes o tránsitos.*
El uso de estos servicios presenta diversos retos de privacidad ya que los proveedores hacen uso de información acerca de la ubicación del usuario, dato exclusivamente de carácter personal. Además, la ubicación del usuario a menudo es registrada sin su consentimiento y, consecuentemente, no es informado del uso que se le va a dar. Parece razonable exigir que estos proveedores informen a los consumidores acerca de esta eventualidad. En otras ocasiones, la aplicación avisa de la recogida de la información de localización, pero la notificación proporcionada no se realiza de forma adecuada o clara. En este artículo se estudia el marco legal aplicable a este tipo de servicios acerca del uso de datos personales y de las notificaciones a los usuarios. Paralelamente, mostraremos cómo tres aplicaciones móviles gestionan los datos de la ubicación de los usuarios y otros datos de configuración del servicio, analizando su comportamiento acerca de la privacidad en la gestión de los datos personales.

ABSTRACT: *Location-Based Services (LBS) offer the users information about their environment, such as nearby restaurant, cinemas, tourist interest points, etc. There are multiple applications related to electronic commerce which embed LBS services. Recently there have been published numerous applications aimed at touristic sector which make use of LBS: Both tourists and citizens demand information related to their position in their trips and commutes.*
The use of these services present several challenges to privacy as providers use information about the location of the user, information that is deemed as personal data. Moreover, the location of a user is frequently collected without his/her consent and, consequently the user is not informed about the uses for this data. It seems reasonable that these providers provide with this information to the consumers. In other occasions, the application warns the user about the gathering of this location information, however, the warning is not necessarily provided to the user in a clear manner. In

this article, we study the legal frame applicable to this kind of services in regards to the collection and notification of this Personal data.
In parallel, we will show how three different mobile applications manage the location of users and other configuration data for the service, analysing how they behave in terms of user's privacy.

PALABRAS CLAVE: Servicios basados en geolocalización, Turismo, Privacidad, Legislación, Seguridad, Datos personales.

KEYWORDS: Location-Based services, Turism, Privacy, Legislation, Security, Personal Data.

1. INTRODUCCIÓN A LOS SERVICOS TURÍSTICOS BASADOS EN GEOLOCALIZACIÓN

Los teléfonos inteligentes, las tabletas y otros dispositivos móviles similares tienen acceso a redes de datos y también son capaces de ejecutar aplicaciones complejas. Además, estos dispositivos implementan sistemas de localización como el GPS o basados en otras técnicas de localización como GSM o Wi-Fi. La combinación de ambas capacidades puede ser útil para construir nuevas aplicaciones basadas en la ubicación del usuario. Estas aplicaciones proporcionan a los clientes del servicio valiosa información relacionada con su ubicación.

Los servicios basados en localización (LBS) son un tipo de servicio ofrecido a los usuarios de dispositivos móviles que proporciona un valor añadido relacionado con el contexto en el que se encuentran los usuarios. Los servicio LBS incluyen diferentes tipos de aplicaciones de comercio electrónico, publicidad, redes sociales generales como Twitter, redes sociales móviles como Foursquare o aplicaciones diversas de Google. Pero el área que puede verse más beneficiado por el uso de LBS es el turismo, debido a sus características especiales. Los turistas suelen exigir los servicios porque no son conscientes de la información relacionada con su entorno, por lo que son un objetivo importante para los LBS.

Las aplicaciones turísticas basadas en localización proporcionan a los viajeros el acceso a la información turística durante sus viajes. Los servicios turísticos que se pueden mejorar mediante el uso de la ubicación del usuario se pueden clasificar en cuatro grupos[1] dependiendo del tipo de servicio:

- Localización de personas y lugares.
- Enrutamiento.
- Búsqueda específica en los alrededores.

[1] S. BERGER, H. LEHMANN, F.LEHNER, "Location-based services in the tourist industry", *Journal of InformationTechnology&Tourism, Vol 5, Num. 4*, 2003, pp. 243-256.

- Información sobre las condiciones del viaje.

También pueden ser clasificados de acuerdo a la fase del viaje en la que se utilizan:

- Planificación / Reserva.
- Transporte.
- Alojamiento
- Información / Apoyo en el destino.

Estas aplicaciones recogen información personal del usuario con el fin de ofrecerle el servicio. Esta información podría ser utilizada para generar un perfil de ubicación del usuario con el fin de conocer sus movimientos habituales. Con el objetivo de utilizar adecuadamente esta información sensible, las solicitudes deben incluir herramientas de configuración, incluyendo la cuestión de solicitar al usuario si permite el uso por parte de la aplicación de sus datos de localización. Es necesario incluir en los LBS los mecanismos que permitan la protección de la privacidad del usuario sin limitar el uso de las aplicaciones.

Estas aplicaciones pueden utilizar tanto la ubicación actual del usuario como el rastro o itinerario de todas sus ubicaciones. Las aplicaciones que utilizan el rastro de los usuarios tienen más requisitos de privacidad.

Este artículo está organizado de la siguiente manera: en la sección 2, se analizan los servicios basados en localización en función de los requisitos de anonimato del usuario y los datos personales recogidos por el proveedor de servicios; la sección 3 abarca la legislación específica para los servicios basados en localización; en la Sección 4 se estudian algunos servicios turísticos representativos del uso de datos de geolocalización, con especial atención a la utilización de los datos personales y la ubicación; en la sección 5 se reanuda la exposición de las preocupaciones relacionadas con la privacidad y la seguridad de los LBS, teniendo en cuenta la legislación descrita anteriormente; por último, la sección 6 presenta las conclusiones.

2. REGISTRO DE DATOS PERSONALES EN SERVICIOS BASADOS EN LOCALIZACIÓN

Un LBS está personalizado cuando el servicio proporcionado tiene en consideración los intereses personales de los usuarios (por ejemplo, información sobre lugares de interés turístico, información detallada de mapas, información de transportes, direcciones o fotos). Es decir, la información geográfica facilitada en un servicio LBS viene condicionada por la voluntad del usuario. Este aspecto constituye una característica fundamental de estos servicios. 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.

Además, algunas aplicaciones turísticas pueden ser vistas como sistemas de información ubicuos adaptativos que tienen acceso a la información pública y personal. Asimismo, pueden adaptar estas informaciones y servicios a cada usuario según su contexto y ubicación actual. En la mayoría de los casos, el modelo de adquisición de datos del usuario se realiza a través del seguimiento de sus actividades y su movilidad geográfica (evaluación del usuario) o por un análisis de las características de su conexión y del dispositivo usado (evaluación del

uso). No obstante, estos procedimientos de recopilación de información pueden afectar de forma dramática a la privacidad de sus usuarios.

En Europa se han puesto en marcha varias experiencias que guardan relación con servicios LBS para proyectos turísticos. Se trata de proyectos como mToGuide (mobileTourism Guide), CRUMPET (CReationofUser-friendly Mobile services PErsonalised for Tourism), PALIO (Personalised Access to Local Information and servicesfortOurists), proyecto GUIDE, LoL@ (Local LocationAssistant), TourServ, I-TOUR (i-TOUR: intelligentTransportsystemfo rOptimizedURbantrips)[2].El caso del proyecto "CRUMPET" se centra en la investigación de servicios móviles personalizados para el turismo. Este proyecto utiliza las nuevas tecnologías como los agentes de software inteligentes y técnicas de modelado de usuario para crear perfiles de usuario. Por lo tanto, hay un servicio y una adaptación de contenidos en función de los intereses individuales de los usuarios por medio del modelado de usuario (utilizando técnicas para la elaboración de perfiles dinámicos de los intereses personales de los mismos). Por lo tanto, para proteger su privacidad es esencial conseguir un diseño equilibrado entre lo que la tecnología puede ofrecer y lo que los usuarios están dispuestos a aceptar. Se trata de evitar que la población tenga malas experiencias al darse cuenta de cómo sus datos que, en principio debieran de mantenerse en privado, de hecho, pueden tener otros usos.

Obviamente, para que cualquier servicio basado en la localización funcione, será necesario que el proveedor de servicios conozca la ubicación del usuario. La precisión dependerá de cada servicio en concreto y del método para obtener la ubicación (es decir, GPS, torres y antenas para redes celulares, puntos de acceso Wi-Fi o dirección IP). No obstante, los usuarios necesitan cierta orientación para determinar si el servicio es aceptable o no desde el punto de vista de la privacidad de los datos recabados. Sólo si se proporciona información adecuada al usuario acerca de los datos de localización recopilados, su almacenado y posterior uso, el usuario puede tomar una decisión razonada de cómo y cuándo utilizar el servicio.

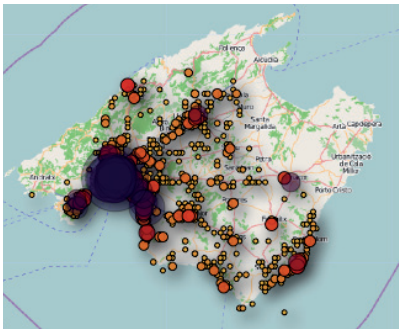
Por ejemplo, los dispositivos de Google y Apple utilizan diversas formas para comunicar la localización del usuario. Respecto a Google, el dispositivo solicita el permiso explícito del usuario cuando éste elige la opción de utilizar Wi-Fi como método de localización. El dispositivo de Google también almacena los datos de localización del usuario por un período limitado y estos datos son encriptados. Sin embargo, los dispositivos Apple tradicionalmente no han pedido explícitamente el permiso para guardar estos datos. Se descubrió que estos dispositivos almacenaban los datos de localización sin cifrar y durante un período largo de tiempo. Se generaba entonces un problema inmediato: los datos se almacenaban de una forma fácilmente legible en la máquina del usuario (es decir, los datos de localización se almacenaban en el ordenador del usuario cuando se sincronizaba con el dispositivo). Los usuarios de iPhone pueden emplear iPhone-Tracker[3], una aplicación de código abierto que lee los mapas con la información que el iPhone ha grabado sobre los movimientos del usuario (Figura 1). Sin embargo, y hasta este momento, no ha habido ninguna evidencia de que estos datos de localización se hayan transmitido más allá del dispositivo del usuario y de los ordenadores utilizados para la sincronización con el móvil.

---

[2] Información sobre detalles de estos proyectos se pueden consultar en URLs:
- http://cordis.europa.eu/result/rcn/29781_en.html
- http://cordis.europa.eu/result/rcn/141312_en.html
- http://www.2020-horizon.com/CRUMPET-Creation-of-user-friendly-mobile-services-personalised-for-tourism%28CRUMPET%29-s47011.html

[3] http://petewarden.github.io/iPhoneTracker/

Figura 1. Captura de pantalla de la aplicación iPhone Tracker: mapa de los movimientos registrados por un iPhone



Podemos analizar la forma diferente de interactuar con el usuario entre los dispositivos de Google y Apple al descargar cualquier aplicación desde la tienda de aplicaciones de cada proveedor. En Android la aplicación tiene la autorización para utilizar estos datos para cualquier fin, siempre y cuando el proveedor de la aplicación pida permiso y los usuarios finales den su aprobación. En los dispositivos de Apple, en cambio, el proveedor de la aplicación tiene que declarar explícitamente con qué finalidad la aplicación necesita saber la ubicación del dispositivo, dejando claro que las aplicaciones no pueden usar esta información de localización con un único fin publicitario. Además, el usuario puede entrar en la ventana de configuración del sistema y comprobar las aplicaciones que actualmente tienen permiso para leer los datos de localización y las aplicaciones que están utilizando el servicio. El enfoque de Android ha llevado a algunas experiencias inapropiadas. Por ejemplo, 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.

Otro caso de controversia en el uso de los datos de localización proviene del mayor fabricante europeo de aparatos de navegación vía satélite para automóviles, la compañía TomTom. El navegador vía satélite del coche de los conductores holandeses que eran dueños de un dispositivo TomTom estaba grabando su datos de localización y los datos agregados a ella, como la velocidad de los coches. Al parecer, esta información era transmitida y supuestamente vendida a la policía holandesa. A continuación, la policía la utilizaba para ajustar los controles de velocidad en las carreteras del país. Al hacerse pública esta conducta, la empresa se vio obligada a disculparse.[4]

La Privacidad de Datos es la adaptación a la sociedad de la información del derecho fundamental a la intimidad y la vida privada. Según varias encuestas llevadas a cabo por Harris Interactive en nombre de TRUSTe[5], la principal preocupación para el 38% de los usuarios de los teléfonos inteligentes es la privacidad. Esta preocupación es mayor entre los usuarios de más edad en comparación con los más jóvenes. La encuesta también muestra que sólo el 25% de los usuarios creen que su tienda de aplicaciones móviles ofrece aplicaciones que protegen su privacidad y sólo el 38% de los usuarios confía en que las aplicaciones, *per se*, ya protegen la privacidad de los usuarios. La mayoría de los consumidores no quieren compartir su ubicación con los proveedores de aplicaciones o sus desarrolladores (77% usuarios dijeron que prefieren no compartir su ubicación con nadie, y sólo el 2% de los encuestados está de acuerdo en compartir sus datos de localización con las compañías desarrolladoras de apps o a terceros).

[4] https://www.youtube.com/watch?v=Zc_cGepf1qg
[5] http://www.truste.com/consumer-privacy/personal-privacy-tips/

En esta encuesta se confirma que la seguridad es una preocupación creciente entre los usuarios de aplicaciones para móviles (por ejemplo, sólo alrededor de un tercio los usuarios sienten que tienen el control de su dispositivo y un 74% de ellos se sienten incómodos con la idea del seguimiento de sus datos para publicidad dirigida). Sólo una minoría de los consumidores piensa que tienen el control sobre la recogida y uso de su información de localización a través de aplicaciones móviles. Así, los consumidores que reciben alertas referentes a "compartir la ubicación" con la compañía desarrolladora de la app son más propensos a permitirlo. En otras palabras, cuando una aplicación requiere tener acceso a los datos basados en la localización, un simple mensaje emergente de petición genera algún tipo de confianza en el usuario que permite el intercambio estos datos. Esta confianza ayudará a difundir el uso de este tipo de aplicaciones, sin embargo, debe de tenerse en cuenta que la confianza en sí misma no es una garantía de privacidad.

3. PRIVACIDAD Y SERVICIOS BASADOS EN LOCALIZACIÓN: ASPECTOS JURÍDICOS Y NORMATIVA APLICABLE

Del análisis que se realiza en este artículo queda patente el uso de datos de localización en diferentes aplicaciones que permiten a los viajeros acceder a información turística durante sus viajes, según su localización: permiten localizar personas y lugares; buscar localizaciones, información sobre las condiciones de viaje, etc. Todo ello partiendo de la localización del usuario y también el itinerario de sus localizaciones. Se trata además de técnicas cada vez más utilizadas por los interesantes resultados que se consiguen.

Sin embargo, la problemática sobre la privacidad de los usuarios salta a primer plano en el campo de los datos basados en localización. Los usuarios deberían saber si sus teléfonos móviles están transmitiendo datos sobre su localización. A partir de aquí se plantean muchas cuestiones, entre ellas: ¿Quién conoce la localización de un determinado usuario? ¿Está informado de forma clara y comprensible del uso de sus datos de localización? ¿Cómo y cuándo debe informarse a los usuarios sobre el uso de sus datos de localización?[6]

El marco normativo, a nivel europeo, se concreta en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009. A nivel nacional, la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPDP) así como la Ley General de Telecomunicaciones.

Según el artículo 3 de la LOPDP se considera dato de carácter personal cualquier información referente a una persona física o jurídica identificada o identificable. El Informe 13/2011 del Grupo de Trabajo del Artículo 29 así lo corrobora[7]. La Directiva 2002/58/CE del Parlamento

[6] *Vid*. A. PANIZA FULLANA, "La publicidad basada en buscadores y "adwords", la reputación on line y el uso de datos de geolocalización", A. PANIZA FULLANA (Coordinación), *Nuevas fórmulas de comercialización on line de servicios turísticos: subsunción en los tipos legales y distribución de responsabilidad*, Granada, 2013, pp. 90 a 93.

[7] Según este Informe y haciendo referencia al nº 4/2007, sobre el concepto de dato de carácter personal, afirma que: *"Smart mobile devices are inextricably linked to natural persons. There is usually direct and indirect identifyability.*

Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 define en su artículo 2 los "datos 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"*. En consecuencia, tendrá que encontrarse necesariamente un equilibrio entre estas técnicas y la privacidad del usuario.

La problemática que genera la cuestión ya queda reflejada en el considerando 35 de la Directiva sobre Privacidad y Comunicaciones Electrónicas. Lo hace en estos términos: *"En las redes móviles digitales se tratan los datos sobre localización que proporcionan la posición geográfica del equipo terminal del usuario móvil para hacer posible la transmisión de las comunicaciones. Tales datos constituyen datos sobre tráfico a los que es aplicable el artículo 6 de la presente Directiva. Sin embargo, además, las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario para la transmisión de comunicaciones y que se utilizan para la prestación de servicios de valor añadido tales como los servicios que facilitan información sobre tráfico y orientaciones individualizadas a los conductores. El tratamiento de tales datos para la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Incluso en los casos en que los abonados hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización"*.

Tanto el artículo 9 de la Directiva sobre Privacidad y Comunicaciones Electrónicas como el artículo 48.2 de la Ley General de Telecomunicaciones establecen el régimen aplicable al uso de datos de localización. Según estas normas, se podrá proceder al uso de datos de localización relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público cuando:

— Los datos de localización se hayan hecho anónimos o previo consentimiento informado del usuario (según el artículo 9 de la Directiva sobre Privacidad y Comunicaciones Electrónicas el proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido).

— Únicamente podrán usarse en la medida y por el tiempo necesario para la prestación de servicios de valor añadido.

First of all, the telecom operator providing GSM and mobile internet access usually has a register with the name, address and banking details of every customer, in combination with several unique numbers of the device, such as IMEI and IMSI.

Secondly, the purchase of extra software for the device (applications or apps) usually requires a credit card number and thereby enriches the combination of the unique number(s) and the location data with directly identifying data.

Indirect identifyability can be achieved through the combination of the unique number(s) of the device, in combination with one or more calculated locations.

Every smart mobile device has at least one unique identifier, the MAC address. The device may have other unique identification numbers, added by the developer of the operating system. These identifiers may be transmitted and further processed in the context of geolocation services. It is a fact that the location of a particular device can be calculated in a very precise way, especially when the different geolocation infrastructures are combined. Such a location can point to a house or an employer. Especially with repeated observations, it is possible to identify the owner of the device".

— Además, el usuario debe tener conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado[8].

— Los usuarios deben tener la posibilidad de revocar su consentimiento otorgado para el tratamiento de los datos de localización distintos de los de tráfico en cualquier momento.

— Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

— En relación al encargado del tratamiento, sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico, personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

Sin embargo, el uso de estos datos pueden plantear nuevos riesgos cuando se combinan con el uso de las redes sociales o se usan para fines comerciales[9]. En el caso de la interacción con las redes sociales se plantean nuevos problemas cómo el de saber quién tiene acceso a esta información.

4. ANÁLISIS DE TRES SERVICIOS BASADOS EN LOCALIZACIÓN Y SUS APLICACIONES MÓVILES

En esta sección vamos a investigar las funcionalidades que proporcionan tres aplicaciones móviles Android basadas en localización y relacionadas con el sector turístico. Se analizará cómo estas aplicaciones realizan el tratamiento de los datos de los usuarios y de qué forma este tratamiento puede afectar a la privacidad de los mismos. Para conocer de cada una de las aplicaciones seleccionadas los permisos que el usuario debe de otorgar, instala-

[8] También se pueden encontrar Guías de Buenas Prácticas en la prestación de servicios basados en datos de localización. Es el caso de la guía "Best Practices and Guide lines for Location-Based Services" de la Wireless Association (http://www.ctia.org/policy-initiatives/voluntary-guidelines/best-practices-and-guidelines-for-location-based-services). En ella encontramos algunas recomendaciones como las siguientes:

"LBS providers must inform users about how their location data will be used, disclosed and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure. Once a user has chosen to use a LBS, or authorized the disclosure of location information, he should be able to choose when or whether location information can be disclosed to third parties and should have the ability to revoke such authorization. LBS providers must inform users about how their location data will be used, disclosed and protected.LBS Providers may use written, electronic or oral notice so long as LBS users have an opportunity to be fully informed of the LBS Provider's information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous".

[9] En el caso de "Yelp": *"When the user is connected, can share his current location, and Yelp responses with a list of near points of interest with comments and evaluations of each local business registered on: search for businesses near you; links to find nearby bars, restaurants, cafes,…; browse reviews to read what's great (and not so great); check-in and share on Facebook and Twitter".*

Y en el caso de "Tripit": *"You can easily share trip plans with family or colleagues directly, or let Facebook and Linkedin contacts know when and where you're headed".*

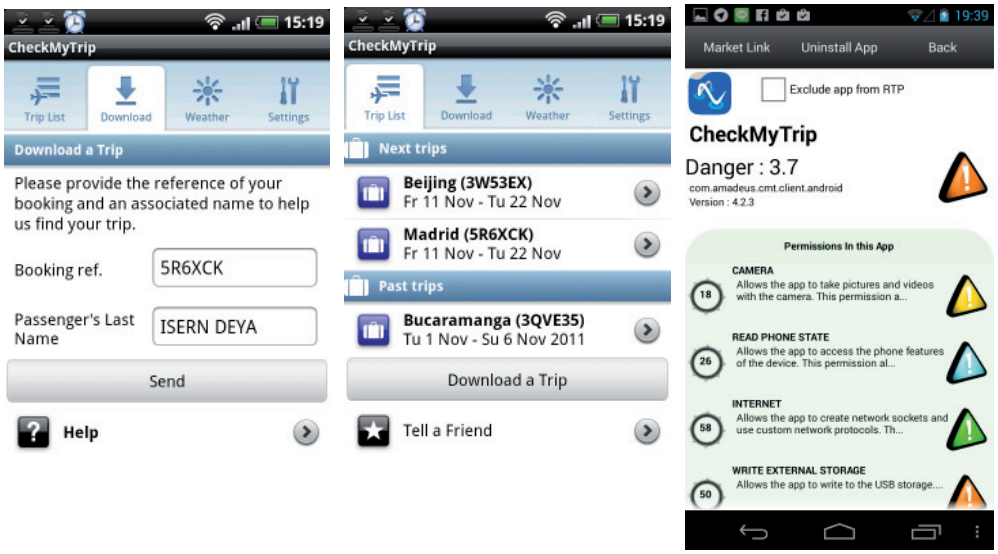
mos una aplicación llamada PermissionDog[10], que determina cuáles son los permisos que requiere una cierta aplicación Android.

4.1. *CheckMyTrip*

La primera aplicación seleccionada es CheckMyTrip, cuyo desarrollador es Amadeus IP Group S.A., empresa líder en los sistemas de distribución global (GDS, Global Distribution System) y el mayor tramitador de reservas para la industria de los viajes y el turismo. Cuando un cliente compra un billete de avión, la aerolínea tramita su reserva y como parte del proceso, Amadeus bloquea la plaza en sus sistemas centralizados. Por tanto, además de la aerolínea interesada, el registro de la compra del billete se almacena también en Amadeus. A partir de esta información, cualquier cliente que haya comprado un billete en una aerolínea asociada con Amadeus, puede acceder al itinerario completo mediante la aplicación CheckMyTrip.

La aplicación móvil requiere solamente que el usuario introduzca el número de reserva y sus propios apellidos para descargar el itinerario (Figura 2). El número de reserva normalmente se envía a través de correo electrónico a la dirección que el cliente proporcionó en el momento de la compra del billete. Cuando el cliente introduce estos dos campos, los datos del itinerario se descargan desde los sistemas de Amadeus y se almacenan en el dispositivo. Los datos descargados son los siguientes (Figura 2): el nombre completo de los viajeros; la agencia o el sitio web dónde se compraron los billetes; las fechas y horas del viaje; el número de reserva; el origen y el destino; los asientos asignados para cada viajero; la duración del viaje; etc.

Figura 2. Ventanas de la aplicación CheckMyTrip y permisos que requiere CheckMyTrip.



La aplicación Android requiere de relativamente pocos permisos para funcionar (Figura 2), de entre los cuales cabe destacar tres permisos con peligro moderado para la privacidad del usuario:

[10] PermissionDog application, available at URL: *https://market.android.com/details?id=com.PermissioDog*

- El acceso a la localización fina (proporcionada por el dispositivo GPS incorporado), usada para para proporcionar a los usuarios información sobre su localización en el aeropuerto.
- La lectura de los contactos almacenados en el dispositivo móvil.
- La lectura de eventos de calendario guardados en el dispositivo móvil, incluyendo tanto los eventos propios como los de los amigos.

Por tanto, de acuerdo con PermissionDog, la aplicación Android de CheckMyTrip presenta un riesgo bajo o moderado de acceso a datos de carácter personal, con una puntuación de 3.7 puntos sobre 5.

4.2. *Yelp*

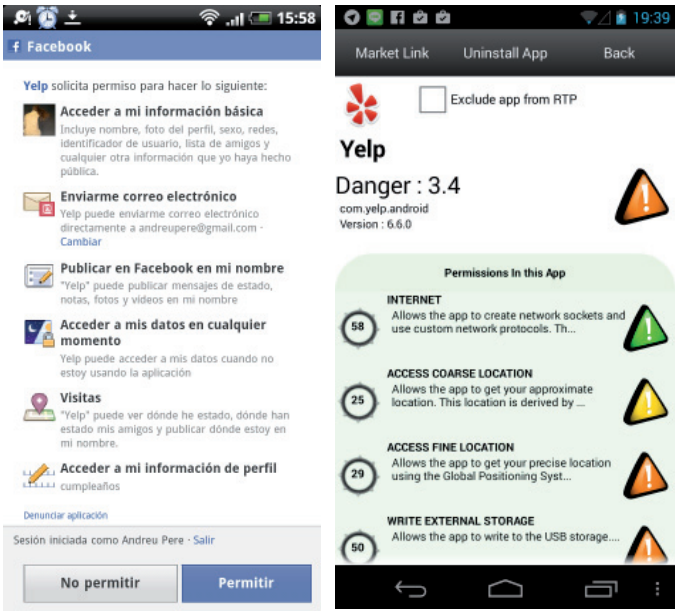
Yelp es una empresa dedicada a publicar opiniones y críticas de negocios locales hechas por los mismos usuarios del servicio. Cuando el usuario visita Yelp, puede buscar restaurantes, cines, dónde comprar, divertirse, etc., y recibir recomendaciones, comentarios y evaluaciones de negocios cercanos, basando la información proporcionada en la localización del usuario.

La aplicación Android de Yelp requiere de once permisos sobre el sistema y los datos del usuario (Figura 3). Por ejemplo, si evaluamos los permisos más sensibles, cabe destacar los siguientes:

- Acceso a la localización aproximada (basada en el uso de la localización a través de la red móvil) y a la localización exacta (usando el GPS).
- Acceso de escritura en la unidad de almacenamiento externa.
- Lectura de todos los contactos almacenados en el dispositivo móvil.

Por tanto, la aplicación presenta un nivel moderado de peligrosidad en la manipulación de datos privados, con una puntuación de 3.4 sobre 5, según la aplicación PermissionDog.

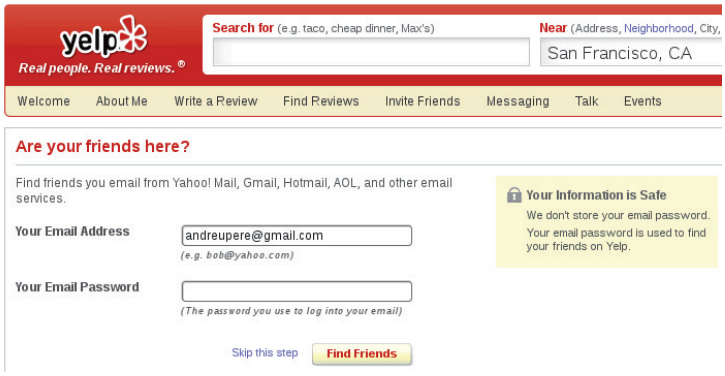
Figura 3. Lista de permisos requeridos por la aplicación Android de Yelp y redirección a Facebook desde la misma aplicación para la aceptación de los permisos de acceso al perfil del usuario en Facebook



Yelp, como tantos otros servicios en Internet, permite enlazar el perfil propio de Facebook con la cuenta en el servicio a través de la aplicación móvil. Yelp redirige al usuario a su perfil de Facebook, a través del cual se presenta la lista de permisos solicitados por el servicio para acceder a las funcionalidades y datos almacenados en Facebook. Entonces, el usuario tiene que aceptarlos todos si quiere terminar con el proceso de unión de perfiles. Yelp pide el acceso a la información básica del perfil (nombre completo, foto, sexo, redes, lista de amigos y otra información publicada por el usuario); a la capacidad de enviar correos electrónicos al usuario; la opción publicar en su nombre (enviar mensajes, notas, fotos y vídeos como si fuera el usuario); el acceso a todos estos datos en cualquier instante (incluso si el usuario no está usando Yelp); y el acceso a los lugares que ha publicado en Facebook (dónde el usuario y sus amigos han estado y Yelp puede publicar dónde está el usuario en su nombre).

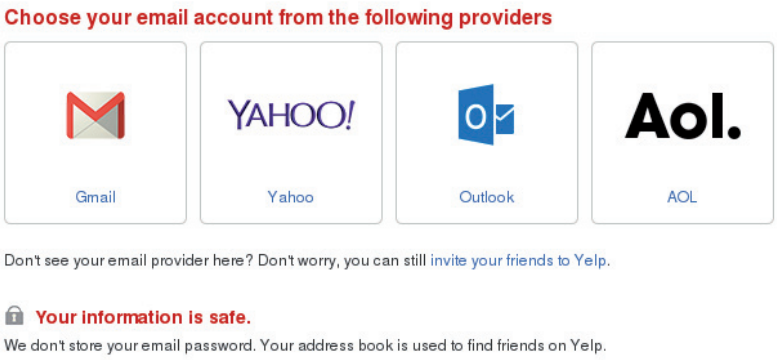
A parte de la aplicación Android, Yelp permite a los usuarios encontrar a los amigos que ya están registrados en el servicio. Hace unos años, esta funcionalidad requería que los usuarios proporcionasen al servicio su dirección de correo electrónico (como por ejemplo Gmail, Yahoo, Hotmail y otros) juntamente con la correspondiente contraseña, para descargar la lista de contactos almacenados (Figura 4). Por tanto, Yelp pedía información privada con la única promesa que no guardaría la contraseña proporcionada por el usuario. Desde el punto de vista legal, en este caso el usuario tenía que proporcionar información privada a terceras partes.

Figura 4. En el pasado, Yelp pedía la contraseña del correo electrónico del usuario para acceder a sus contactos



Actualmente, Yelp ha mejorado la privacidad de este proceso, de modo que el servicio ya no pide la contraseña de la cuenta de correo electrónico del usuario, sino que redirige al proveedor de correo correspondiente (Figura 5). Es éste proveedor quién proporciona los datos a Yelp, después de presentar al usuario una pantalla de aceptación dónde le informa que Yelp ha solicitado permiso para acceder a su cuenta y con qué propósitos lo va a hacer.

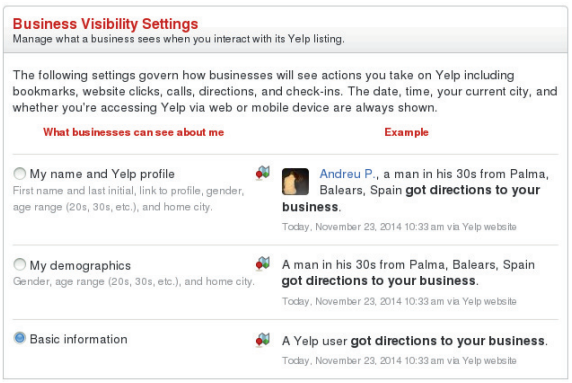
Figura 5. Actualmente, este proceso de búsqueda de contactos ha mejorado y la privacidad de los usuarios se ve más protegida



A parte del aumento de la privacidad que acabamos de comentar, Yelp también ha mejorado la personalización de los datos del usuario que se muestran públicamente en el perfil del servicio. Así pues, actualmente el servicio da la posibilidad al usuario de elegir entre tres niveles de divulgación de datos (Figura 6):

- En la primera opción, la información publicada es el perfil completo.
- En la segunda opción, ya no aparece el nombre del usuario ni la fotografía de perfil, por tanto, la información pública se ha transformado en parcialmente anónima.
- En la última opción, el perfil solo muestra información básica sin datos personales concretos que puedan ser usados para la identificación del usuario.

Figura 6. Opciones de privacidad en Yelp acerca de cómo presentar el perfil público del usuario



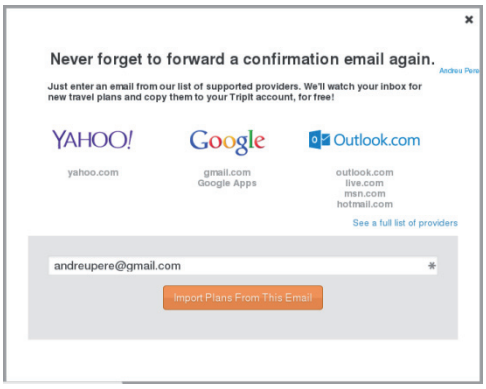
4.3. *TripIt*

TripIt es un servicio que automáticamente captura todos los detalles de los viajes a partir de los correos electrónicos de confirmación que remiten las compañías al usuario y crea el itinerario detallado de cuándo y a dónde viaja el usuario.

TripIt proporciona dos métodos de importación de correos de confirmación. La primera opción es manual, en la que el usuario reenvía el correo de confirmación a una dirección de

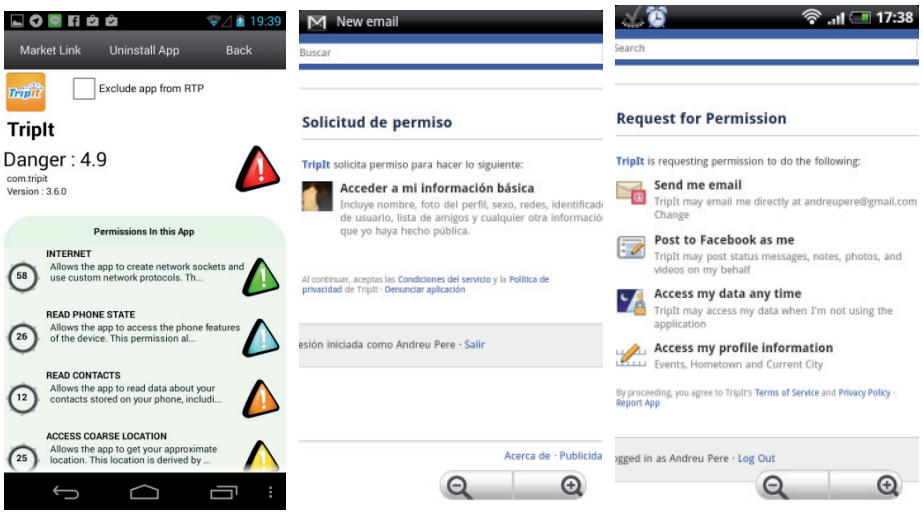
correo electrónico de TripIt. Entonces, a su recepción, el servicio crea automáticamente el itinerario y lo añade al perfil del usuario. La segunda opción disponible para importar los itinerarios no requiere de ningún tipo de intervención por parte del usuario. TripIt analiza todos los correos contenidos en una cuenta de correo electrónico del usuario (por ejemplo, de Gmail) buscando correos que contengan datos de confirmaciones de viajes y reservas. Para conseguir acceder a la cuenta de correo electrónico, TripIt pide a los usuarios permiso para importar planes de viaje desde su cuenta, así como acceder a la lista de contactos almacenada en cada proveedor (Figura 6). Por tanto, está claro que para importar datos, TripIt debe leer todo el correo del usuario para determinar cuáles se corresponden con planes de viajes, pudiendo esta funcionalidad ocasionar un grave problema de privacidad para el usuario.

Figura 7. Pantalla en TripIt requiriendo el acceso a los correos del usuario en Gmail



TripIt también permite enlazar cuentas de usuario con el correspondiente perfil de Facebook de forma similar al procedimiento explicado anteriormente en el caso de Yelp (Figura 8). Si el usuario decide aceptar todos los permisos requeridos, entonces TripIt puede empezar a extraer información de Facebook o leer los contactos, e incluso notificarles sobre nuestros planes de viaje. Los permisos solicitados para acceder a la información del perfil de Facebook son los siguientes: enviar correos electrónicos directamente desde su correo electrónico; enviar mensajes de estado, fotos y vídeos al perfil de Facebook como si fuera el usuario y sin su intervención; acceso a sus datos en cualquier momento aunque el usuario no utilice la aplicación; y acceso a la información de su perfil, como eventos y lugar de residencia.

Figura 8. Permisos requeridos por TripIt en Facebook y permisos otorgados a la aplicación Android



Finalmente, en los términos y condiciones, TripIt indica que todos los datos recopilados sobre planes de viaje pueden ser usados para propósitos comerciales, como pueden ser recomendaciones y anuncios relacionados con el viaje. Por tanto, esto significa que TripIt puede enviar algunos datos a terceras partes, como anunciantes, al tiempo que el servicio puede conseguir interesantes ingresos a cambio de estos datos.

En relación a los permisos requeridos por la aplicación Android, se puede observar que de las tres aplicaciones y servicios analizados, TripIt es la aplicación que presenta un riesgo más alto, con una puntuación de 4.9 sobre 5 según el análisis de PermissionDog (Figura 8). En total, requiere la aceptación de hasta 25 permisos, de los cuáles un buen número pueden ser considerados peligrosos:

- Acceso a la localización aproximada y completa del usuario.
- Acceso de lectura y escritura a la agenda propia y de los contactos.
- Acceso de lectura y escritura a la lista de contactos.
- Capacidad de realizar llamadas telefónicas sin la intervención del usuario.
- Acceso de lectura y escritura a todos los dispositivos de almacenamiento.

Todo lo comentado plantea una serie de cuestiones importantes desde el punto de vista legal. El uso de los datos personales, tales como datos de localización o datos contenidos en correos electrónicos y en el mismo dispositivo, requieren el cumplimiento de la Ley de Protección de Datos: consentimiento del usuario, información previa sobre el uso de los datos, etc. En este caso, TripIt puede acceder al contenido de los correos electrónicos del usuario, así como a su lista de contactos, hecho que puede afectar seriamente a la privacidad del usuario. Por otro lado, en el caso del envío de datos a terceras partes, el objetivo de tal envío debe de estar directamente relacionado con el consentimiento dado por el usuario y atendiendo a las finalidades del mismo. De otro modo, no puede obtenerse el consentimiento del usuario solo aceptando los términos general y las condiciones del servicio electrónico de comunicaciones ofrecido.

A raíz del análisis presentado, se puede comprobar como hay aplicaciones que requieren la aceptación por parte del usuario de unos permisos que a veces no tienen relación con el servicio que se va a prestar. Este hecho puede deberse a diferentes motivos: a la programa-

ción de la misma aplicación (interesada o no) o al encadenamiento de permisos que fuerza el sistema operativo, ya que existen permisos que requieren implícitamente el cumplimiento de otros. En relación a los permisos requeridos por una aplicación, cabe reclamar la necesidad de permitir al usuario de una aplicación la capacidad de elegir qué permisos quiere otorgar y qué otros no. Así pues, el usuario tiene que aceptar todos los permisos si quiere usar una aplicación, y no tiene la posibilidad de elegir una aceptación parcial de los permisos. Por tanto, sería muy interesante llegar a la situación en la que la negación a un permiso únicamente impidiera la ejecución de una función específica que requiere de ese permiso en particular.

5. DATOS DE LOCALIZACIÓN: PUNTOS CLAVE PARA LA PROTECCIÓN DE LA PRIVACIDAD DEL USUARIO

De la normativa aplicable a los datos de localización así como los informes del Grupo de Trabajo del artículo 29[11] se puede extraer que:

— Es necesario obtener el consentimiento del usuario para el uso de datos de localización para ofrecer servicios de valor añadido. Este consentimiento tiene que ser previamente informado y específico para los usos o finalidades para los que se van a utilizar los datos de localización.

— Los proveedores de servicios de valor añadido deben adoptar las medidas necesarias para obtener el consentimiento de los usuarios en los términos establecidos en las normas; evitándose usos fraudulentos.

— Tal como se ha establecido en el documento del Grupo de trabajo del artículo 29: *Opinion 13/2011 on geolocation services on Smart mobiledevices,* el consentimiento para el uso de datos de geolocalización no puede obtenerse a través de la aceptación de un clausulado de condiciones generales.

— Los documentos del Grupo de Trabajo del artículo 29 se decantan por el sistema *opt in* para obtener el consentimiento del usuario para utilizar los datos de geolocalización. Por otra parte es el que ya se impuso para el envío de comunicaciones comerciales.

6. CONCLUSIONES

Los servicios basados en localización serán cruciales en el desarrollo de aplicaciones turísticas. Esta tecnología es capaz de añadir información valiosa relacionada con el entorno en el que los usuarios están situados. Sin embargo, el servicio puede vulnerar la privacidad de los usuarios. Es necesario, por tanto, que las nuevas aplicaciones tengan en consideración el marco legal aplicable a los servicios basados en localización. En este artículo hemos analizado la forma que tienen algunas aplicaciones de manejar los datos de localización. A

[11] *Vid.* S. CAVANILLAS MÚGICA, "Nuevas formas de promoción y contratación de servicios turísticos en Internet", A. PANIZA FULLANA (Coordinación),*Nuevas fórmulas de comercialización on line de servicios turísticos: subsunción en los tipos legales y distribución de responsabilidad*, Granada, 2013, página 20.

partir de aquí, identificamos la necesidad de desarrollar aplicaciones que proporcionen la información de una forma satisfactoria al usuario en base a los datos de localización que van a ser tratados, almacenados y usados, así como las finalidades y los usos concretos de estos datos. En caso contrario, los servicios turísticos basados en localización podrían no cumplir con lo establecido en el marco normativo existente.