Nota informativa

Autoridades europeas de protección de datos aprueban un Dictamen sobre el impacto en la privacidad de los servicios de geolocalización de Smartphones

- **El Dictamen analiza los riesgos de estos servicios para la privacidad de sus usuarios, el marco jurídico aplicable y las garantías que los proveedores de servicios de geolocalización en dispositivos móviles deben cumplir.**
- **Destacan que los datos de localización de smartphones pueden revelar detalles íntimos sobre la vida privada de su propietario, y permitir obtener patrones de conducta del titular del dispositivo para crear perfiles.**
- **De forma predeterminada, los servicios de localización deben estar apagados, y su activación requerirá del consentimiento informado y específico del usuario.**
- **Los interesados deben poder retirar su consentimiento de manera fácil, sin ningún tipo de consecuencias negativas para el uso de su dispositivo.**

(Madrid 18 de mayo de 2010). Las Autoridades Europeas de Protección de Datos (Grupo de Trabajo del Artículo 29) han aprobado **un Dictamen** sobre la incidencia y los riesgos para la privacidad **de los "Servicios de Geolocalización en dispositivos móviles inteligentes**", en el **que establecen el marco jurídico aplicable**, en materia de protección de datos, a los servicios de geolocalización disponibles en los dispositivos móviles inteligentes, como son, entre otros: los mapas y los servicios de navegación, los servicios geopersonalizados (incluidos los puntos cercanos de interés), la realidad aumentada, el geoetiquetado de contenido en Internet, el seguimiento del paradero de los amigos, el control infantil o la publicidad basada en la localización.

El Dictamen analiza los tres principales tipos de infraestructuras destinadas a prestar servicios de geolocalización-GPS, estaciones base GSM y WiFi- así como los principales responsables que recopilan y tratan datos de localización obtenidos a partir de los dispositivos móviles y entre los que se incluyen los proveedores de la infraestructura de geolocalización, fabricantes de teléfonos inteligentes y los desarrolladores de aplicaciones basadas en geolocalización.

Riesgos para la privacidad

Las Autoridades de protección de datos destacan el impacto que pueden tener en la privacidad de los usuarios los Servicios de Geolocalización debido a que la tecnología de dispositivos móviles inteligentes- Smartphones- **permite la monitorización constante de los datos de localización**; a que los dispositivos están íntimamente ligados a una persona concreta; y a que normalmente existe una identificabilidad directa e indirecta del usuario.

En este sentido, el llamado Grupo de Trabajo del Artículo 29 destaca que esta tecnología, que puede llegar **a revelar detalles íntimos sobre la vida privada de su**

propietario, permite a los proveedores de servicios de geolocalización **una visión personal de los hábitos y los patrones del propietario del dispositivo y creen perfiles exhaustivos,** que pueden también incluir categorías especiales de datos- si por ejemplo, revelan las visitas a los hospitales y los lugares de culto, la presencia en las manifestaciones políticas o de presencia en otros lugares específicos que revela datos sobre la vida sexual ejemplo-.

Asimismo, destacan que los usuarios de este tipo de dispositivos **pueden no ser conscientes de que envían su ubicación ni de a quién lo hacen, ni para qué,** y que el consentimiento que otorguen para que determinadas aplicaciones utilicen sus datos de localización puede no ser **válido, ya que la información que se otorga en ocasiones al usuario es incomprensible, está obsoleta o, es inadecuada.**

Además, las Autoridades alertan de otros de los riesgos que pueden plantearse para la privacidad derivados de la **desviación de finalidad en el uso de los datos de localización.**

Obligaciones. Consentimiento informado y específico

Respecto a los requisitos para conciliación de estos de estos servicios con la Directiva de protección de datos, las Autoridades europeas de protección de datos establecen que **el principal fundamento** para que el tratamiento de los datos de localización sea legítimo **es el consentimiento previo e informado.**

En este sentido establecen que **de forma predeterminada, los servicios de localización deben estar apagados** y que la activación de estos servicios **requiere de un consentimiento informado y especifico a los diferentes fines para que los datos sean captados o almacenados.** La i**nformación debe ser clara, completa y comprensible** para un público general que no disponga de conocimientos técnicos y deberá poder accederse a la misma de forma continuada y sencilla.

Asimismo se destaca que **el consentimiento no se puede obtener a través de la aceptación obligatoria de los términos y condiciones generales,** y que los usuarios deben **ser capaces de retirar su consentimiento de una manera fácil**, sin ningún tipo de consecuencias negativas para el uso de su dispositivo.

También, el Grupo de Trabajo recomienda **limitar el alcance del consentimiento en términos de tiempo y recordárselo a los usuarios por lo menos una vez al año.** Además, en el caso de una suscripción regular a un servicio de geolocalización, para **evitar el riesgo de que se realice una monitorización de los datos de localización en secreto**, se considera que es fundamental que **el dispositivo advierta continuamente que la función de geolocalización está activada,** por ejemplo, a través de un icono que se encuentre permanentemente visible.

Por otra parte, sobre **la utilización de esta tecnología en el ámbito laboral** se destaca que, respecto a los trabajadores, los empresarios sólo podrán adoptar esta tecnología cuando pueda demostrarse que es necesaria para un fin legítimo. En los casos en los que pueda justificarse debidamente, el empresario debe buscar siempre los medios menos intrusivos, evitar la monitorización constante e informar a los trabajadores sobre como desactivar el dispositivo de monitorización fuera de las horas de trabajo.

Respecto su utilización para el **control infantil,** los padres deben juzgar si el uso de este tipo de aplicaciones está justificado en circunstancias específicas. **Como mínimo,**

deben informar a sus hijos y, tan pronto como sea posible, deben permitirles tomar parte en la decisión de utilizar este tipo de aplicación.

Periodo conservación de los datos
El Dictamen establece que los proveedores de servicios y aplicaciones de geolocalización deben implementar políticas de conservación de los datos que garanticen que tanto los datos de geolocalización como los perfiles que se creen a partir de los mismos, se eliminen **tras un periodo justificado de tiempo.**

Entre otras consideraciones respecto a la conservación de datos el Dictamen también señala que si el desarrollador del sistema operativo o el responsable del servicio de geolocalización demuestra que es necesario recoger el histórico de los datos **para actualizar o mejorar el sistema,** ha de implantar las máximas garantías para evitar que esta información se haga identificable.

Derechos de los usuarios
El Dictamen subraya que los proveedores de servicios de geolocalización y las aplicaciones deben respetar y cumplir **los derechos de los usuarios a acceder,** rectificar o borrar, **los datos de ubicación que se han recogido,** a los posibles perfiles sobre la base de éstos datos de localización, así como información sobre destinatarios a quienes se comuniquen los datos. La información debe facilitarse en un formato legible.

El Dictamen integro puede consultarse en:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

Grupo de trabajo del Artículo 29
El Grupo de Trabajo del Artículo 29 es el grupo consultivo compuesto por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. El Grupo de trabajo del artículo 29 está facultado para examinar cualquier cuestión que esté relacionada con la aplicación de las directivas en materia de protección de datos para contribuir a la aplicación uniforme de las mismas. Desempeña sus funciones emitiendo recomendaciones, dictámenes y documentos de trabajo sobre todas aquellas cuestiones relevantes que afectan a la protección de datos personales.

Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y el artículo 15 de la Directiva 2002/58/CE.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm