

Expediente N°: E/06697/2017

## **RESOLUCIÓN DE ARCHIVO DE ACTUACIONES**

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad GOOGLE LLC, de oficio y en virtud de denuncia presentada por la ASOCIACIÓN PARA LA PREVENCIÓN Y ESTUDIO DE DELITOS, ABUSOS Y NEGLIGENCIAS EN INFORMÁTICA Y COMUNICACIONES AVANZADAS (APEDANICA), y teniendo como base los siguientes

### **HECHOS**

**PRIMERO:** Con fecha 23/11/2017, la Directora de la Agencia Española de Protección de Datos acordó iniciar actuaciones de investigación a la entidad Google LLC (antes Google Inc.), en lo sucesivo GOOGLE, en relación con los datos que recaba y los tratamientos que realiza sobre la información que proporciona la ubicación de los terminales móviles.

Con fecha 26/11/2017, la Asociación para la Prevención y Estudio de Delitos Abusos y Negligencias en Informática y Comunicaciones Avanzadas (APEDANICA) presentó una denuncia sobre estos mismos hechos, indicando que los terminales con el sistema “Android” permiten que GOOGLE acceda a todo tipo de datos y metadatos sin control. Añade dicha entidad que Google ha reconocido el acceso masivo al geoposicionamiento de personas que utilizan este tipo de Smartphone

APEDANICA manifiesta que hay publicaciones en diversos medios de comunicación de Internet respecto de estos hechos e indica la url <http://www.abc.es/tecnologia/abci-aunque-desactives-movil-google-conoce-ubicacion-exacta-cada-momento-201711212118.html> como ejemplo de una de ellas.

**SEGUNDO:** La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Con fecha 04/12/2017, por la Inspección de Datos se accedió a la dirección aportada por APEDANICA, <http://www.abc.es/tecnologia/abci-aunque-desactives-movil-google-conoce-ubicacion-exacta-cada-momento-201711212118.html>, verificando que consta una noticia sobre la recopilación de datos de localización de las personas con dispositivos Android que GOOGLE realiza desde principios del año 2017.

En la noticia publicada, de fecha 21/11/2017, se informa además que no es obligatorio tener activado el dispositivo, porque GOOGLE puede conocer una ubicación más o menos exacta de dónde se encuentra a través de las antenas con las que los dispositivos se conectan. Asimismo, informa que GOOGLE ha admitido esta práctica aunque manifiesta que no se han utilizado los datos registrados, que se encuentran encriptados y son inaccesibles para terceros.

2. Con fecha 11/12/2017, por la Inspección de Datos se comprobó la existencia de diversas noticias respecto de estos hechos, publicadas en diferentes medios en Internet en fecha 21/11/2017:

- 2.1. <http://www.elmundo.es/tecnologia/>.
- 2.2. <https://www.elconfidencial.com/tecnologia/>
- 2.3. <https://culturacolectiva.com/tecnologia>
- 2.4. <https://xalaka.com/privacidad/>

Todas ellas se hacen eco de la noticia e indican que GOOGLE no niega esta práctica, aunque manifiesta que se ha utilizado para mejorar las notificaciones y los mensajes que reciben los móviles *Android* y que, desde finales de noviembre, los teléfonos *Android* dejaron de enviar información.

3. Con fecha 11/12/2017, se requirió información a GOOGLE y de la respuesta recibida en fecha 01/02/2018 se desprende lo siguiente:

- 3.1. GOOGLE manifiesta que:

*La información publicada en medios de comunicación versa sobre el código del lado del dispositivo (device-side code), que es parte del sistema empleado por Google para asegurar que los dispositivos mantienen una conexión constante con los servidores, de modo tal que puedan recibir notificaciones y mensajes en tiempo real.*

*El sistema determina el intervalo óptimo en el que los dispositivos deben "contactar" (hacer ping) con los servidores para asegurar que esa conexión constante se mantenga abierta.*

*En caso de que se corte la conexión, puede retrasarse la recepción de los mensajes y notificaciones, y los usuarios tendrían que "refrescar" sus dispositivos para recibir nuevos mensajes. Este sistema está diseñado para ayudar a los usuarios: la determinación del intervalo óptimo permite conservar la batería de sus dispositivos y asegurar a la vez que la mensajería instantánea permanece disponible.*

*Mientras que el código del lado del dispositivo (device-side code) transmite datos que incluyen el Código Indicativo del País para el Servicio Móvil (Mobile Country Code - MCC), el Código Indicativo de Red para el Servicio Móvil (Mobile Network Code -MNC) y otra información como el número único asignado a cada torre móvil (Cell ID); el código del lado del servidor (server-side code) tan solo registra el MCC y el MNC.*

GOOGLE manifiesta que no se ha producido seguimiento de la localización de los dispositivos que han descrito los medios de comunicación y que las informaciones sobre la utilización de los datos de *Cell ID* procedente de las transmisiones de los dispositivos para rastrear ubicaciones de los usuarios son infundadas y falsas. Añade que los datos tratados por GOOGLE en el contexto de este sistema se limitan a los necesarios para lograr el objetivo de optimizar las conexiones de mensajería instantánea.

- 3.2. Añade GOOGLE que su Política de Privacidad (disponible en <https://www.google.com/intl/es/policies/privacy/>) informa que trata "información de la

*red móvil*" de los dispositivos de los usuarios. Los usuarios de terminales móviles *Android* con servicios de GOOGLE deben confirmar que conocen y aceptan la Política de Privacidad antes de utilizar su dispositivo *Android*. De conformidad con la citada Política de Privacidad, GOOGLE utiliza la información de la red móvil para "*proporcionar, mantener... y mejorar*" los servicios que se prestan a los usuarios de terminales móviles *Android*.

GOOGLE manifiesta que la base legitimadora consiste en mantener las conexiones para facilitar la mensajería instantánea y para mejorar y aumentar la calidad y fiabilidad del servicio. Los datos recogidos se encuentran agregados y pseudonimizados y la finalidad del tratamiento se encuentra estrictamente delimitada a tablas que contienen información relativa al país y a la red.

- 3.3. Asimismo, informa que la funcionalidad tratada consiste en un sistema de sincronización de redes que fue lanzado a través de un programa piloto de prueba y se implementó por fases. A principios de enero de 2017, se implantó a un porcentaje reducido de usuarios de *Android*, y se completó en febrero de 2017.

Dicho sistema de sincronización de redes es facilitado por GOOGLE para dar soporte a la mensajería instantánea en aplicaciones propias y de terceros en dispositivos "*Android*" (ej., chat o notificaciones). El mismo es capaz de determinar con qué frecuencia debe un dispositivo enviar una señal para mantener activa la conexión con los servidores (depende del país -MCC-, la red móvil de conexión -MNC- y la torre móvil -Cell ID).

El código del lado del dispositivo (*device-side code*) de los terminales móviles *Android* está diseñado para transmitir información desde el dispositivo, que incluye estos tres elementos. El Cell ID no se haya incluido entre los datos que GOOGLE registra en sus servidores para el sistema de sincronización de redes.

El código del lado del dispositivo (*device-side code*) transmite un conjunto de elementos de datos ligeramente distinto en función de la red móvil incluyendo un identificador (ID) del dispositivo *Android* y un *token* de autenticación, que son utilizados para garantizar la seguridad y legitimidad de la conexión y para que se envíe la información correcta al dispositivo adecuado.

Estas transmisiones se envían a través del protocolo *TCP/IP* desde los dispositivos *Android* al servidor de sincronización de notificaciones de Google y a través de una conexión permanentemente cifrada.

El sistema de sincronización de redes se apoya también en el código del lado del servidor (*server-side code*), que determina qué información registra Google en sus servidores para utilizarla como parte del sistema de sincronización de redes. A este respecto, Google manifiesta que el código de los servidores de Google está configurado para registrar únicamente datos relativos a MCC y MNC, descartando los datos de Cell ID.

Google manifiesta que el sistema de sincronización de redes nunca ha registrado ni utilizado datos de Cell ID de las transmisiones para calcular intervalos de envío de señal (*heartbeat ping*) ni para rastrear la ubicación de los usuarios.

## **FUNDAMENTOS DE DERECHO**

### **I**

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

### **II**

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), establece:

*“Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.”*

### **III**

El artículo 6.1 de la LOPD dispone lo siguiente: *“El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”.*

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en aquel apartado 1, estableciendo que: *“No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”.*

Estos preceptos, a su vez, se encuentran desarrollados por el artículo 10 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en el que se establece lo siguiente:

*“Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.*

- 1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.*
- 2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando;*

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

*El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.*

*El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.*

b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

*No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley.*

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

*Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.*

*Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.*

*La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.*

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

*En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".*

En el presente caso, las actuaciones de investigación se inician en relación con la recogida de información por parte de GOOGLE sobre la ubicación de dispositivos móviles “Android”, obtenida a través de las antenas con las que dichos dispositivos se conectan.

Dichas actuaciones han determinado que GOOGLE únicamente almacena datos del país (MCC) y de la red móvil de conexión (MNC), pero no de la torre móvil (cell-id). Esta información es transmitida por los terminales y utilizada para establecer las conexiones, pero no se registra en los servidores de la entidad ni se usa para rastrear la ubicación de los usuarios.

Se tiene en cuenta que esa información se utiliza con la finalidad de sincronizar la conexión de los dispositivos móviles Android con los servidores, posibilitando la recepción de notificaciones y mensajes en tiempo real en los terminales. Es decir, GOOGLE sólo utiliza datos de ubicación para la remisión de mensajes.

De este modo, resulta que la finalidad de la recogida de aquella información no es obtener información relativa a las personas ni el tratamiento posterior de dicha información, sino que la finalidad última es la prestación de servicios.

Por lo tanto, el tratamiento de datos que conlleva la sincronización de redes, en la medida en que está vinculado a la prestación de servicios de mensajería instantánea libremente aceptados por el usuario, se encuentra amparado por las normas reseñadas anteriormente.

En consecuencia, no existen indicios sobre un posible incumplimiento por parte de GOOGLE de la normativa de protección de datos, sin perjuicio de que si de cualquier información sobrevenida, se pudiera deducir un eventual incumplimiento, se activen las actuaciones inspectoras pertinentes, con los efectos que en cada caso se determinen.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

**SE ACUERDA:**

**PROCEDER AL ARCHIVO** de las presentes actuaciones.

**NOTIFICAR** la presente Resolución a GOOGLE LLC, a través de GOOGLE SPAIN, S.L., y a la entidad ASOCIACIÓN PARA LA PREVENCIÓN Y ESTUDIO DE DELITOS, ABUSOS Y NEGLIGENCIAS EN INFORMATICA Y COMUNICACIONES AVANZADAS (APEDANICA).

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de

octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Mar España Martí  
Directora de la Agencia Española de Protección de Datos