



Expediente Nº: E/01104/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de denuncia presentada por **A.A.A.** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 08/01/2018, tuvo entrada en esta Agencia escrito de D. **A.A.A.** (en lo sucesivo el denunciante), en el que denuncia a FACEBOOK, por los siguientes hechos:

A pesar de tener restringido a Facebook el acceso a los datos personales de su terminal móvil (fotos, geolocalización, etc.), éste viola continuamente dichas restricciones proponiéndole la publicación en su perfil de fotografías almacenadas en su terminal o notificándole la bienvenida a ciudades que visita.

Dice haber activado la restricción del acceso a través de la configuración de seguridad de Android.

Facebook le sugiere publicar fotos almacenadas en su terminal, y cuando lo hace, aparece la foto con un texto en el que se indica que solo las ve el usuario del mismo.

SEGUNDO: Tras la recepción de la denuncia 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:

Con fecha 28/02/2018 y 01/03/2018 se han realizado las siguientes pruebas con ayuda de un terminal móvil de la Subdirección General de Inspección, de marca Samsung y modelo Galaxy A3 (SM-A300FU), versión de Android 6.0.1 y nivel de parche de seguridad de Android 1 de Junio de 2017 (versión software de seguridad ASKS v1.2_161011).

Se han descargado del Play Store la aplicación FACEBOOK (versión 161.0.0.35.93), así como la aplicación MESSENGER (versión 155.0.0.14.93) y se han instalado en el terminal móvil. El motivo de haber instalado esta segunda aplicación es que en las impresiones de pantalla adjuntadas por el denunciante se observa el icono de la aplicación en las dos, y en previsión de que fuera la interacción de ambas la causante de los hechos denunciados, se han realizado pruebas con y sin la aplicación MESSENGER instalada.

Se han observado los siguientes hechos:

1. En el apartado relativo a los Permisos de la aplicación FACEBOOK y MESSENGER, en la sección “Administrador de Aplicaciones” del área “Ajustes”, se pueden activar o desactivar los permisos relativos a “Almacén”, “Ubicación” y “Cámara”.
2. Si “Almacén” y “Ubicación” se encuentran desactivados, no se ha conseguido que FACEBOOK o MESSENGER accedan a fotografías del terminal móvil o a la

geolocalización del mismo sin generar una ventana emergente en la que se pida el permiso al usuario. Sin embargo, se ha comprobado que en el supuesto de que MESSENGER hubiera estado activado en el pasado inmediato y su permiso “Ubicación” acabara de haber sido desactivado, al intentar registrar la ubicación para enviarla en un mensaje se visualiza el fragmento de mapa que se había cargado cuando el permiso de “Ubicación” estaba activado. Se puede comprobar que es solo ese fragmento de mapa el que se visualiza, y no se dibuja el punto exacto donde se localiza el terminal. Si se intenta ir más allá, solo se ven zonas en blanco rellenas con cuadrículas.

3. Para poder utilizar la funcionalidad de cámara en FACEBOOK, es necesario que esté activado el permiso “Cámara”. MESSENGER necesita que adicionalmente esté activado el permiso “Micrófono”.
4. No se ha observado que la activación de los permisos analizados en MESSENGER altere el comportamiento de las funcionalidades de FACEBOOK, en lo tocante a acceso a recursos del terminal móvil o la geolocalización del mismo.
5. En la sección de “Seguridad” del área de “Ajustes” del terminal, no se encuentra ningún apartado adicional donde se puedan configurar los mencionados permisos de acceso al almacén o a la ubicación.
6. En la sección de “Ubicación” del área de “Ajustes”, existe un interruptor en la esquina superior derecha que permite desactivar la funcionalidad de Ubicación del terminal móvil para todas las aplicaciones instaladas en él. Si se desactiva la funcionalidad desde aquí, FACEBOOK y MESSENGER (CONFIRMAR LA 2ª) dejan de tener acceso a la ubicación. Si se activa en alguna de ellas (intentando registrar la ubicación y contestando afirmativamente a la pregunta de confirmación), se queda activado en el terminal móvil para todas las aplicaciones.

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

En el presente caso, el denunciante ha manifestado que tiene restringido el acceso de Facebook a sus datos personales a través de su terminal; no obstante, aunque Facebook le notifica que no le ha dado permiso para localizarle, recibe constantemente sugerencias para publicar sus fotos, visitas a ciudades, compras, etc, considerando que su privacidad e información están siendo vulneradas.

En primer lugar, hay que señalar que pese a las actuaciones de investigación llevadas a cabo por la Inspección de Datos no se ha podido constatar lo expresado por el afectado en su escrito de denuncia.

En segundo lugar, el denunciante no ha aportado pruebas de que Facebook este queriendo acceder a los recursos de su terminal móvil, ni instándole a su publicación. De las impresiones de pantalla aportadas en su escrito de denuncia la primera de ellas se refiere a una fotografía que acaba de capturar y a la que le puede añadir efectos visuales. No aparece una fotografía procedente de lo que se conoce como *Galería* del móvil. Tampoco justifica que Facebook este intentado acceder a la misma ni que la aplicación le esté proponiendo publicarla.

Así, de las pruebas y comprobaciones llevadas a cabo tanto el 28/02/2018 como el 01/03/2018 con la ayuda de un terminal de la propia Inspección se ha verificado lo siguiente:

Desactivando los permisos *Almacen* y *Ubicación* de la aplicación desde la sección "*Administrador de Aplicaciones del área de Ajustes*", Facebook Messenger impide el acceso a los recursos del almacenamiento del terminal móvil y la geolocalización del mismo. El comportamiento general es generar una ventana emergente donde se pide permiso para activación proporcionando las dos opciones de *rechazar* o *permitir* o una sola *aceptar*.

Tampoco se ha logrado reproducir la función consistente en sugerir la publicación de fotografías, sino que es el usuario el que debe *clikear* en el área correspondiente para publicar un mensaje, fotografía video, etc.

En relación con las impresiones de pantalla aportadas por el denunciante, no se ha conseguido reproducir el mensaje "*Solo tú puedes ver esto*" de la primera de ellas, ni tampoco la notificación "*Facebook is denied to obtain your current posición*" de la segunda.

Por otra parte, se desconoce a qué se quiere referir el denunciante con la expresión "*Configuración de seguridad de Android*", ya que en la sección de "*Seguridad*" no se ha encontrado ningún apartado para permisos de acceso a *almacén* o a *ubicación*.

Por último, se desconoce la versión Facebook Messenger que posee el denunciante así como el sistema operativo Android de su terminal, pues tampoco se puede olvidar que existen aplicaciones que con el tiempo son corregidas por versiones posteriores lo que complica la posible constatación de los hechos denunciados.

En definitiva, pese a las actuaciones de investigación llevadas a cabo por la Inspección de Datos no se ha podido constatar los hechos que se denuncian en relación con la plataforma de red social Facebook a través de internet.

En este orden de ideas debe tenerse en cuenta que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, teniendo plena virtualidad el principio de presunción de inocencia, que debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetado en la imposición de cualesquiera sanciones. Esto, porque el ejercicio del *ius puniendi*, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones.

En tal sentido el Tribunal Constitucional, en Sentencia 76/1990, considera que el derecho a la presunción de inocencia comporta *“que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio”*.

Como ha precisado el Tribunal Supremo en STS de 26 de octubre de 1998 la vigencia del principio de presunción de inocencia “no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

Por su parte el Tribunal Constitucional en STC 24/1997 ha manifestado que *“los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

- a) La prueba indiciaria ha de partir de hechos plenamente probados.*
- b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras).”*

A la luz de lo expuesto se concluye que el principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo que acredite los hechos que motivan la imputación o la intervención en los mismos del presunto infractor. Trasladando los razonamientos precedentes al supuesto que nos ocupa, habida cuenta de que no se ha podido constatar los hechos denunciados, conducta que pudiera ser constitutiva de una infracción de la LOPD, corresponde acordar el archivo de las actuaciones de investigación practicadas.

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

SE ACUERDA:

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

NOTIFICAR la presente resolución a la entidad **FACEBOOK INC.**, en su domicilio social, y también a través de **FACEBOOK SPAIN, S.L.** como establecimiento del responsable en España para que dé traslado de la misma a **FACEBOOK INC** y a **A.A.A.**.

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