Procedimiento Nº: E/01873/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante CAMBIDGE ANALYTICA, FACEBOOK INC., FACEBOOK IRELAND LIMITED, FACEBOOK SPAIN, S.L., y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 5 de abril de 2018 la Directora de la Agencia Española de Protección de Datos acuerda iniciar las presentes actuaciones de investigación en relación a que datos privados de usuarios de la red social Facebook fueron utilizados por CAMBRIDGE ANALYTICA para manipular psicológicamente a los electores, en las elecciones a Presidente de Estados Unidos celebradas en el año 2016, y existe la posibilidad de que haya habido destinatarios del servicio de Facebook afectados por esta utilización de datos que radiquen en España.

Posteriormente, con fechas de entrada 11 y 12 de abril de 2018, se presentan denuncias sobre estos mismos hechos por parte de CONFEDERACIÓN DE CONSUMIDORES Y USUARIOS y ASOCIACION DE CONSUMIDORES Y USUARIOS EN ACCION -FACUA*,* respectivamente, los que ponen de manifiesto la aparición de noticias en medios de comunicación informando de que el número de afectados en España por la cesión de datos de usuarios de Facebook sin consentimiento recogidos por CAMBRIDGE ANALYTICA puede llegar hasta los 137.000.

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

1- En la fecha del 14/06/2018, tiene entrada escrito presentado en nombre de FACEBOOK IRELAND LIMITED en respuesta a requerimiento de información a FACEBOOK SPAIN, S.L. Y se anexa, entre otra, la siguiente documentación relevante para esta investigación:

1. Se manifiesta que los datos de los usuarios de Facebook fueron recabados por una aplicación denominada “thisisyourdigitallife”, que se dio de alta en la Plataforma de Facebook en **noviembre de 2013**, desarrollada por el ***DR. A.A.A.*** y su empresa ***Global Science Research Limited (GSR)***, que posteriormente facilitaron dichos datos a varias entidades, entre las que se encuentra ***SCL***, que es la matriz de ***Cambridge Analytica***.

2. Se manifiesta que, en el momento en que se produjo la cesión de datos, Facebook Login permitía a los desarrolladores solicitar el consentimiento a los usuarios para acceder a información que habían compartido con esos usuarios sus amigos de Facebook.

3. Se manifiesta que Facebook tuvo conocimiento de la cesión de datos entre el ***DR. A.A.A.*** y ***Cambridge Analytica*** a través de un artículo publicado en el diario *The Guardian* el **11/12/2015**, y revocaron los derechos de acceso de la aplicación "thisisyourdigitallife" a Facebook Login el **17/12/2015**.

4. Se manifiesta que hubo 44 personas en España que se instalaron la aplicación "thisisyourdigitallife", y que hay 136.941 personas en España que, pese a no haberse instalado la aplicación, tenían amigos que sí se la habían instalado y su configuración de seguridad permitía el acceso de la aplicación a sus datos.

5. Se manifiesta que, en una declaración ante la Comisión para Asuntos Digitales, Culturales, Medios de Comunicación y Deportes de la Cámara de los Comunes del Reino Unido, el ***DR. A.A.A.*** indicó que se produjo una transmisión de datos entre ***GSR*** y ***SCL*** de acuerdo con un contrato entre ambas partes, y que, de acuerdo con dicho contrato, se transmitieron datos únicamente de participantes en el estudio y de sus amigos en once estados de Estados Unidos: Arkansas, Colorado, Florida, Iowa, Luisiana, Nevada, New Hampshire, Carolina del Norte, Oregón, Carolina del Sur y Virginia Occidental.

6. Se manifiesta que la forma en que las aplicaciones de terceros pueden solicitar permisos a los usuarios de Facebook para acceder a sus datos es a través de una interfaz de programación de aplicaciones (en adelante, API) proporcionada por Facebook, cuyo uso está sujeto a cumplir con la "Política de la Plataforma de Facebook".

7. Se manifiesta que las aplicaciones implementadas sobre la versión 2 de la Plataforma de Facebook desde el inicio a los siguientes datos de los usuarios que les hubiesen dado permisos: perfil público del usuario, dirección de correo electrónico y lista de amigos que también utilizan dicha aplicación. Si estas aplicaciones pasaban un procedimiento de comprobación denominado "App Review", podían obtener permisos para acceder a más información.

8. Se manifiesta que la versión 2 de la Plataforma de Facebook se comenzó a utilizar en **abril de 2014**.

9. Política de datos de Facebook revisada el **15/11/2013**, en la que se indica, entre otras cosas, lo siguiente (es traducción): "*si compartes cualquier información en Facebook, cualquiera que pueda verla puede compartir dicha información con otros, incluyendo los juegos, aplicaciones y sitios web que use."*

10. Política de datos de Facebook revisada el **30/01/2015**, en la que se indica, entre otras cosas, lo siguiente (es traducción): "*Cuando te descargas o utilizas*

servicios de terceros, estos pueden acceder a tu Perfil Público, que incluye tu nombre de usuario o identificación de usuario, tu rango de edad, tu país/idioma, tu lista de amigos, así como cualquier información que compartas con ellos. La información recabada por estas aplicaciones, sitios web o servicios integrados está sujeta a sus propios términos y políticas".

2- En la fecha del 14/06/2018, tiene entrada escrito presentado en nombre de la INFORMATION COMMISIONER'S OFFICE de Reino Unido en respuesta a requerimiento de información. Y se anexa, entre otra, la siguiente documentación relevante para esta investigación:

1. "Notice of Intent" dirigida a Facebook, en la que se indica, entre otras cosas, que (es traducción de la Agencia):

    a. "*En abril de 2014, las compañías de Facebook introdujeron cambios en la Plataforma de Facebook, que redujeron la capacidad de las aplicaciones para acceder a la información tanto de los usuarios de Facebook como de sus amigos. Para las aplicaciones que ya existían, hubo un periodo de gracia de un año (hasta mayo de 2015) antes de que estuvieran sujetas a estas nuevas restricciones, y, por lo tanto, seguían teniendo la capacidad de recoger los datos de los amigos de los usuarios del mismo modo que antes de abril de 2014 hasta un año después de los cambios*".

    b. "*El **DR. A.A.A.** solicitó migrar la aplicación [*"thisisyourdigitallife"*] a la versión 2 de la API de la plataforma antes del final del periodo de gracia. La aplicación se revisó el 6 de mayo de 2014 y Facebook rechazó la petición del **DR. A.A.A.** para utilizar permisos adicionales al día siguiente.*"

    c. "*Después de mayo de 2014, la aplicación dejó de tener acceso a la información detallada sobre los amigos de sus usuarios, y tuvo acceso a un conjunto de información más limitado sobre sus usuarios. Sin embargo, cuando las limitaciones comenzaron a tener efecto en mayo de 2015, después del periodo de un año de gracia, los desarrolladores de aplicaciones, incluidos del **DR. A.A.A.** y **GSR** podían seguir almacenando la información detallada sobre los usuarios de sus aplicaciones y sus amigos que ya hubieran recogido previamente a través de sus aplicaciones. Las compañías de Facebook no les requirieron en ese momento que borraran dichos datos, o parte de ellos.*"

    d. "*La aplicación continuó activa en la Plataforma de Facebook hasta diciembre de 2015*".

3- En la fecha del 17/08/2018, se consulta en la página de la "Companies House" (Agencia del Gobierno del Reino Unido encargada del registro mercantil) la situación

mercantil de la empresa CAMBRIDGE ANALYTICA (UK) LIMITED. Y se obtiene, entre otra, la siguiente información:

1. La compañía se encuentra en estado "*in Administration*" (que es una situación derivada de un proceso de insolvencia).
2. En la naturaleza de la compañía se indica "*Dormant company*", que indica que la empresa no tiene actividad.

4- En la fecha del 29/08/2018, se consulta la Política de Datos de Facebook en la dirección https://www.facebook.com/privacy/explanation. Esta Política de Datos contiene, entre otra, la siguiente información:

1. La fecha de la última revisión de la Política de Datos es el 19/04/2018.
2. Dentro del apartado "*Retención de datos y desactivación y eliminación de cuentas*", se indica lo siguiente: "*Cuando eliminas tu cuenta, eliminamos el contenido que has publicado, como tus fotos y actualizaciones de estado, por lo que no podrás recuperar esa información. En cambio, la información sobre ti que han compartido otras personas no se eliminará, ya que no forma parte de tu cuenta.*" (el subrayado es de la Agencia).
3. Dentro del apartado "*¿Cómo utilizamos esta información?*", se indica que "*Usamos la información de la que disponemos (de acuerdo con las decisiones que tomes) según lo descrito a continuación para proporcionar los Productos de Facebook y los servicios relacionados descritos en las Condiciones de Facebook y las Condiciones de Instagram, así como para asegurar su funcionamiento.*" (el subrayado es de la Agencia). Después, se indican los fines para los que se utilizan los datos, y, dentro del fin "*Proporcionar, personalizar y mejorar nuestros Productos*", se explican qué categorías de datos se utilizan para este fin, entre las que se encuentra la "*Información relacionada con la ubicación*" y se explica cómo se recaba esta información de la siguiente manera: "*Este tipo de información puede basarse en datos como la ubicación precisa del dispositivo (si nos has permitido recopilar esta información), direcciones IP e información de uso de los Productos de Facebook (como visitas y eventos a los que asistes).*" (el subrayado es de la Agencia).

5- En la fecha del 29/08/2018, se consulta la Política de la plataforma de Facebook en la dirección https://developers.facebook.com/policy/, que contiene las normas que tienen que cumplir los terceros que desarrollan aplicaciones que se integran con la plataforma de Facebook. Esta política contiene, entre otra, la siguiente información:

1. Dentro del apartado "*2. Dar a las personas el control*", se indica, entre otras, la siguiente indicación (el subrayado es de la Agencia):

> *8. Obtén el consentimiento adecuado de las personas antes de usar cualquier tecnología de Facebook que nos permita recopilar y tratar sus datos, como nuestros SDK o píxeles para navegadores. Cuando uses este tipo de tecnología, proporciona un aviso adecuado sobre*

divulgación de contenido en el que indiques:

a. La existencia de terceros, incluido Facebook, que pueden usar cookies, balizas web y otras tecnologías de almacenamiento para recopilar o recibir información de tus sitios web, aplicaciones y otros lugares de internet, y que pueden utilizar esta información para proporcionar servicios de medición y segmentación de anuncios, tal como se describe en nuestra Política de datos.

b. La forma en la que los usuarios pueden negarse a que su información se recopile y utilice a efectos de segmentación de anuncios y el lugar desde el que pueden acceder al mecanismo para ejercer dicha opción.

2. Dentro del apartado "*4. Fomentar un uso correcto*", está, entre otras, la siguiente indicación: "*No modifiques o traduzcas ningún SDK o sus componentes; tampoco crees obras derivadas de ellos ni les apliques ingeniería inversa*".

3. Dentro del apartado "*7. Información que debes tener en cuenta*", está, entre otras, la siguiente indicación: "*Podemos analizar tu aplicación, tu sitio web, tu contenido y tus datos con cualquier fin, incluido el comercial.*".

   En este mismo apartado, se indica lo siguiente: "*Podemos aplicar medidas contra tu aplicación o sitio web si concluimos que has infringido nuestras condiciones o influyes negativamente en la plataforma; asimismo, podemos suspender tu aplicación o sitio web, con o sin previo aviso, mientras investigamos supuestas infracciones de nuestras condiciones. Cabe la posibilidad de que no te informemos por anticipado de dichas medidas […] Las medidas, que pueden tomarse de forma manual o automática, pueden incluir inhabilitar la aplicación, restringiros a ti y a la aplicación el acceso a funciones de la plataforma, obligarte a eliminar datos, rescindir los acuerdos que hayamos firmado contigo o cualquier otra medida que consideremos oportuna.*".

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (en adelante RGPD) reconoce a cada autoridad de control, y en virtud de las funciones establecidas en el art. 12.2 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

Con carácter previo al análisis de la adecuación la normativa de protección de datos de carácter personal es preciso abordar el elemento temporal en el que suceden los hechos objeto de investigación.

La noticia en los medios de comunicación de la filtración de datos de usuarios de la red social Facebook (la red social en lo sucesivo) a través de la entidad Global Science Research Limited (GSR) con destino CAMBRIDGE ANALYTICA es de fecha 11/12/2015 (*artículo publicado en el diario The Guardian*) y los hechos se estiman que se pudieron producir desde la fecha en que la aplicación denominada "thisisyourdigitallife" se dio de alta en la Plataforma de Facebook en noviembre de 2013, hasta la fecha en que se denegó el acceso a la citada plataforma en el mes de diciembre de 2015.

El RGPD establece en su artículo 99 bajo la rúbrica "*Entrada en vigor y aplicación* "lo siguiente:

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.

2. Será aplicable a partir del 25 de mayo de 2018.

Por lo tanto, los hechos que motivan el inicio de las presentes actuaciones de investigación y por tanto el objeto de análisis en el presente procedimiento se producen antes de la plena aplicación del RGPD y por tanto la adecuación a la normativa aplicable debe referenciarse respecto de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD en lo sucesivo).

III

Disponen los artículos 6.1 y 11.1 y 3 de la LOPD lo siguiente:

Art. 6 LOPD (…)*1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa*. (…)

Art. 11 LOPD (…)*1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*

(…)*3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar*. (…)

En el presente caso, resulta que para utilizar la aplicación "thisisyourdigitallife", siendo su función principal la realización de un test de personalidad, los usuarios de la red social prestaban el consentimiento para que los responsables de la aplicación accedieran a determinados datos del perfil de usuario, *como por ejemplo, el contenido en el que se había utilizado el botón "Me gusta",*

actualizaciones de estado, la ciudad dónde estaban o residían, y la identidad de aquellos perfiles que estaban en la lista de amigos.

En concreto en el apartado 6 de las condiciones de uso de la aplicación se hacía constar (…) *information collected: we collect any information that you choose to share with us by using the application. This may incluide, inter alia, the name, demographics, status updates and Facebook likes of your profile and of your network* (…).

De los términos de uso, no se definía la posibilidad de acceder, por ejemplo, a publicaciones, mensajes y múltiple información de otros usuarios que formaran parte de la lista de amigos, ya que indicar "*your network"* tiene un contenido abierto, heterogéneo y sujeto a múltiples interpretaciones, que no permite otorgar un consentimiento informado del usuario– para una finalidad determinada, y que a priori era la realización de un test de personalidad-, ni menos aun de los "amigos" de éste en la red social.

Tampoco se advertía de la posibilidad de que los datos a los que se accediera por parte del desarrollador de la aplicación en cuestión fueran a ser transmitidos a terceras entidades, como sucedió con CAMBRDIGE ANALYTICA, por tanto, cualquier consentimiento otorgado en esas condiciones deviene nulo.

Por lo expuesto, el tratamiento de los datos de los usuarios de la red social Facebook, en relación con la aplicación "thisisyourdigitallife", no encuentra acomodo en los supuestos que permiten el tratamiento y en su caso la cesión de los datos, de acuerdo con los artículos 6 y 11 de la LOPD arriba transcritos.

IV

Acreditada la no adecuación del tratamiento objeto de análisis a la LOPD, y sin perjuicio del análisis posterior que se realiza sobre la prescripción y la afectación de los usuarios españoles, es preciso poner de manifiesto la responsabilidad y culpabilidad en lo sucedido, de la red social Facebook y las empresas que utilizan la plataforma de dicha red social, como fue el caso de Global Science Research Limited (GSR). Para ello debe distinguirse dos estadios en las cesiones producidas. El primero entre la red social y los desarrolladores, y el segundo entre éstos y terceras entidades.

En relación con el principio de responsabilidad, dispone el artículo 28.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, *1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa.*

En relación con el principio de culpabilidad, la Sentencia de la Audiencia Nacional de 17 de octubre de 2007 (Rec. 63/2006) indica: "…*el Tribunal Supremo*

viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto".

En este sentido conviene indicar que, desde el punto de vista material, la culpabilidad consiste en la capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico. Por tanto, lo relevante es la diligencia desplegada en la acción por el sujeto, lo que excluye la imposición de una sanción, únicamente en base al mero resultado, es decir al principio de responsabilidad objetiva. Por eso, es preciso indicar que FACEBOOK es la entidad que establece las normas que tienen que cumplir los terceros que desarrollan aplicaciones – como GSR - que se integran con la plataforma de Facebook y en su caso, establecer unas medidas de control y supervisión.

En concreto en los apartados 5.2 y 5.3 del antecedente segundo de la presente resolución, se establecen normas, y las posibles consecuencias en caso de incumplimiento de las mismas, respecto de las que tienen que cumplir los desarrolladores de aplicaciones cuando utilizan la plataforma FACEBOOK.

Normas que se muestran insuficientes dado el análisis del primer estadio, de la cesión de datos producida. A la vista de la documentación obrante en el expediente, no puede convenirse que FACEBOOK tiene el control –ni si quiera el conocimiento-, desde el inicio hasta el final, de la utilización de los datos de los usuarios de su red social que realizan las terceras empresas desarrolladoras de aplicaciones.

Las cláusulas de la determinación de lo que pueden hacer o no los desarrolladores, no pueden operar como una suerte de exención de responsabilidad en favor de FACEBOOK, que le es propia una diligencia en el tratamiento que se haga de los datos de sus usuarios. Es decir, FACEBOOK no puede situarse en una ignorancia deliberada por aplicación de unas normas de conducta que recomienda que sigan los desarrolladores que utilicen su plataforma y accedan a datos personales de sus usuarios.

Asimismo, debe tenerse en cuenta que la información que se cita en el antecedente segundo es incorporada al expediente a fecha 29/08/2018, y por tanto, con posterioridad a los hechos concernientes a la cesión realizada a través de la aplicación *"thisisyourdigitallife".* Es decir, a la fecha de implementación de esa política de uso, FACEBOOK ya era conocedora de lo sucedido y sus repercusiones, y de la escasa supervisión y control de lo que hacen los terceros desarrolladores y a pesar de ello, las medidas adoptadas o a adoptar que se definen en la política de uso, no minimizan los riesgos de que en la actualidad volvieran a producirse hechos similares.

La política de uso citada centra únicamente el control de la red social en la siguiente información o advertencia (…) *Podemos aplicar medidas contra tu aplicación o sitio web si concluimos que has infringido nuestras condiciones o influyes negativamente en la plataforma; asimismo, podemos suspender tu aplicación o sitio web, con o sin previo aviso, mientras investigamos supuestas infracciones de nuestras condiciones. Cabe la posibilidad de que no te informemos por anticipado de dichas medidas […] Las medidas, que pueden tomarse de forma manual o automática, pueden incluir inhabilitar la aplicación, restringiros a ti y a la aplicación el acceso a funciones de la plataforma, obligarte a eliminar datos, rescindir los acuerdos que hayamos firmado contigo o cualquier otra medida que consideremos oportuna*.". (…)

Teniendo en cuenta lo anterior y en relación con el principio de responsabilidad y culpabilidad, la cesión de los datos producida tiene su origen en un primer estadio, en la deficiente supervisión de FACEBOOK sobre la manera en que los desarrolladores de aplicaciones acceden a los datos de los usuarios. Sin perjuicio de que, una vez producido el acceso, -en un segundo estadio de la cesión-, el tercero desarrollador (GSR en el caso analizado) venda, comunique, o realice cualquier tratamiento de los datos a los que haya accedido, de lo que es obviamente responsable.

Finalmente indicar, que la última actualización de la política de uso, de los desarrolladores que utilizan la plataforma de FACEBOOK es de fecha posterior a la entrada en vigor del RGPD, sin que se haya acreditado en las actuaciones de investigación realizadas, que, a partir de esa fecha, que se produzcan cesiones de datos que tengan relación con el diseño, supervisión y control por parte de la citada red social.

V

En el presente caso la solución procedente en Derecho es el archivo de las actuaciones contra FACEBOOK y CAMBRDIGE ANALYTICA, en la medida en que los hechos objeto de análisis han prescrito (artículo 47 de la LOPD), y en atención a que si bien hubo 44 personas en España que se instalaron la aplicación "thisisyourdigitallife", y que hay 136.941 personas en España que, pese a no haberse instalado la aplicación, tenían amigos que sí se la habían instalado y su configuración de seguridad permitía el acceso de la aplicación a sus datos, lo cierto es que no se ha constatado que los datos de éstos hayan sido comunicados por GSR a CAMBRIDGE ANALYTICA.

En primer lugar, para determinar la prescripción de la infracción que pudiera haberse cometido debe indicarse que la infracción por la vulneración del artículo 6 está prevista en el artículo 44.3 b) de la LOPD y la infracción por la vulneración del articulo 11 está prevista en el artículo 44.3 k) de la LOPD, ambas consideradas como infracción grave, cuyo plazo de prescripción es de dos años de acuerdo con el artículo 47 de la LOPD.

En la medida en que se desconoce en qué fecha concreta se produce la cesión y hasta cuando se produce el tratamiento inconsentido de los datos, no puede determinarse con absoluta precisión el *dies a quo* del inicio del cómputo del citado plazo de dos años. Únicamente se tiene conocimiento que el acceso por parte de GSR a la plataforma FACEBOOK se podía producir hasta el mes de diciembre de 2015, por lo que a fecha de diciembre de 2017 los hechos habrían prescrito.

En segundo lugar, respecto de la no constatación de que los hechos hayan afectado a usuarios españoles, dicha circunstancia obedece que tal como se indica en el punto 3 del antecedente segundo de la presente resolución, la entidad CAMBRDIGE ANALYTICA habría cesado su actividad impidiendo cualquier acción tendente a verificar que dispone o ha dispuesto de datos de carácter personal de usuarios españoles.

VI

No obstante lo anterior, debe indicarse que tras la entrada en vigor del RGPD, las entidades obligadas, deben cumplir sus principios y mandatos, entre los que debe destacarse para el caso analizado, tanto el principio de *responsabilidad proactiva* previsto en el artículo 5.2 del RGPD, como los previstos en el Artículo 25 RGPD relativos a la "*Protección de datos desde el diseño y por defecto*", en el sentido de configurar el servicio de uso de la plataforma Facebook por desarrolladores de aplicaciones, para que no se produzcan de nuevo los hechos analizados, e integrar las garantías necesarias en el tratamiento- *cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad* - a fin de cumplir los requisitos del RGPD y proteger los derechos de los interesados.

Por lo tanto, de acuerdo con lo señalado, y conforme a lo establecido en el art. 60.8 del RGPD, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente resolución al reclamante e **INFORMAR** de ella al responsable del tratamiento.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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 de la referida Ley.

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