Expediente Nº: E/02525/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **TWITTER SPAIN, S.L** como consecuencia del conocimiento de un fallo de seguridad y en base a los siguientes,

HECHOS

PRIMERO: El 05/05/2018 la Directora de la Agencia Española de Protección de Datos acordó las presentes actuaciones de investigación en relación a la noticia difundida por los medios de comunicación, por la recomendación realizada por la red social Twitter a sus más de 330 millones de usuarios, disponible en la dirección *https://blog.twitter.com/official/en_us/topics/company/2018/keepingyour-account-ecure.html*, para que cambien sus contraseñas como medida de precaución, después de que un fallo técnico provocara que algunas de las contraseñas se almacenaran de forma *"no oculta"* en su sistema informático, tal y como explica Twitter en su publicación.

Asimismo, el 04/05/2018, tuvo entrada en esta Agencia escrito de D. ***A.A.A.*** (en lo sucesivo el reclamante) en el que denuncia a **TWITTER SPAIN, S.L**., por los siguientes hechos: la red social facilita información inadecuada sobre cookies afectando a los usuarios y no usuarios de la red, tampoco identifica con claridad los usos y socios que pueden utilizar la información de las cookies, etc., además, podría haber comprometido las contraseñas de millones de usuarios.

Según manifiestan los representantes de **TWITTER SPAIN, S.L.**, la investigación realizada en relación con la brecha en las contraseñas de los usuarios permite realizar las siguientes conclusiones:

a. Fecha y hora en que se produjo

La investigación ha mostrado que el problema fue debido a un cambio en la programación realizado por el equipo de tráfico de Twitter en noviembre de 2016 en el Twiter Front End (TFE).

b. Cómo se produjo

El cambio realizado sobre el procedimiento para registrar información en el TFE tuvo el inintencionado efecto de introducir un error que de forma inadvertida capturó las contraseñas en texto simple mientras estaban siendo comunicadas entre los sistemas en determinadas circunstancias.

c. Tratamiento o ficheros de datos personales afectados

Registros de contraseñas en texto simple en el log TFE.

d. Cuantificación del número de registros (contraseñas) y categorización de los datos personales comprometidos

Aproximadamente 900 millones de contraseñas fueron almacenadas de forma desenmascarada durante la existencia del error informático. Sin embargo, esto no

representa necesariamente el número de cuentas involucradas porque las contraseñas desenmascaradas fueron registradas cada vez que se introducía una contraseña a través de una interacción con el TFE.

e. Número y tipología de usuarios afectados. Número de usuarios españoles afectados

Twiter no está en posición de estimar qué número de contraseñas puede corresponder a usuarios españoles.

f. Posibles causas de la brecha

El error en las contraseñas fue introducido de forma inadvertida mediante el equipo de tráfico de Twitter en noviembre de 2016, a la hora de introducir un cambio en el sistema de registro interno.

g. Identificación de accesos no autorizados, posibles o ciertos, a dicha información no cifrada

No se ha encontrado ningún indicio de que haya habido algún empleado que descargase o copiase sin autorización.

Twitter ha adoptado múltiples acciones de relevancia en pro de su investigación.

Primero, el equipo de compliance de Twitter ha realizado entrevistas a los empleados que consultaron los registros afectados durante el período de tiempo en cuestión, para asegurarse de que cada empleado tenía un fin profesional legítimo para realizar dicha consulta.

Segundo, Twitter ha revisado las comunicaciones de los correspondientes empleados para determinar si alguna contraseña en texto simple ha sido transmitida vía email o por otros medios.

Tercero, Twitter ha realizado una auditoría completa de todos los dispositivos Google Drive desde diciembre de 2016 hasta hoy, para determinar si algún empleado hizo un mal uso o recabó los datos en cuestión.

Cuarto, Twitter ha estado revisando sus registros (logs), por ejemplo, aquellos en los cuales los empleados consultaron los campos en cuestión en los registros afectados que contenían contraseñas en texto simple, para determinar si dichos individuos se estaban potencialmente dirigiendo a o buscando las contraseñas dentro de dichos registros.

Y, por último, Twitter desarrolló una rigurosa búsqueda para identificar áreas donde los empleados hayan podido copiar o acceder a los datos en cuestión de forma voluntaria o involuntaria.

Mientras estas investigaciones están en curso, todas las acciones que Twitter ha adoptado indican que los registros afectados no han sido descargados o copiados de forma inapropiada.

h. Consecuencias de la brecha

Twitter ha contratado forenses externos para investigar si las contraseñas en texto simple fueron compartidas o reveladas con algún tercero.

3. Medidas de seguridad adoptas o propuestas por el responsable del fichero para poner remedio a la brecha de seguridad, incluyendo las adoptadas para mitigar los posibles efectos negativos.

Después de identificar la causa raíz de por qué las contraseñas estaban siendo registradas en texto simple, Twitter introdujo una reparación.

Una vez se completó la reparación, el equipo de seguridad de cuentas, el equipo de tráfico y el equipo de seguridad de la información realizaron un riguroso proceso de validación para confirmar la solución del problema que había sido identificado.

Los ingenieros y abogados de Twitter identificaron una larga lista de medidas para su remedio.

Posteriormente Twitter estuvo escribiendo, testando y validando el código para depurar los registros; proceso detallado y meticuloso en tanto que cualquier error menor podía corromper los registros en su totalidad.

Una vez completado el diseño, el plan de testado, y el código para el proceso de limpieza, Twitter comenzó a borrar los datos de los sistemas de registro. Posteriormente, el 25/04/2018, después de someterse a un complejo proceso de verificación, Twitter fue capaz de confirmar que las contraseñas en texto simple de usuarios había sido completamente eliminado de los registros.

4. Detalle de los tratamientos de datos personales realizados en la compañía, distinguiendo aquéllos de los que son responsables y aquellos que realizan por cuenta de TWITTER INC como encargado del tratamiento. Descripción de la relación con dicha compañía.

Según indican los representantes de la entidad **TWITTER SPAIN, S.L.** no es responsable ni encargado del tratamiento de los datos de los usuarios de los servicios Twitter establecidos en España. Twitter International Company, que es una entidad constituida en Irlanda, y domiciliada en Dublín, presta los servicios Twitter a las personas residentes en España.

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 2.1 de la LOPD, relativo a su ámbito de aplicación, establece:

"1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".

Por otra parte, el artículo 9 de la LOPD establece en relación con la seguridad de los datos que:

"*1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

III

En el presente caso, las actuaciones de investigación tienen lugar como consecuencia, no solo de la denuncia presentada, sino que también es consecuencia de noticias e informaciones difundidas en medios de comunicación ante la recomendación efectuada por la red social TWITTER aconsejando a sus más de 330 millones de usuarios para que cambiaran sus contraseñas como medida de precaución ante un fallo técnico detectado.

TWITER es una red social en línea que permite a los usuarios enviar y leer mensajes cortos de 140 caracteres llamados *"tweets"*. Los usuarios registrados pueden leer y publicar tweets, pero los que no están registrados sólo pueden leerlos. Los usuarios acceden a Twitter a través de la interfaz web, SMS o aplicación para dispositivo móvil.

Hay que señalar, del conjunto de hechos y circunstancias constatadas en el presente caso y analizadas las razones manifestadas por TWITER en su escrito de fecha 11/06/2018 en relación con la investigación realizada como consecuencia de la brecha se seguridad producida en ficheros que albergaban las contraseñas de los usuarios, que el problema fue debido a un cambio en la programación realizado por el equipo de trafico de TWITER en noviembre de 2016 en el sistema interno de autenticación de usuarios, habiendo sido afectados ficheros que contenían las contraseñas de los mismos.

De manera ágil TWITER adoptó numerosas acciones para el esclarecimiento de los hechos y tratar de poner remedio a la situación provocada por la brecha de seguridad motivada por el cambio en el sistema de registro interno, introduciendo nuevas medidas técnicas y que sometidas a un complejo proceso de testificación y verificación, TWITER fue capaz de confirmar que las contraseñas en texto simple de los usuarios había sido completamente eliminado de los registros.

Por otra parte, a pesar de la quiebra detectada no se han encontrado indicios de los que se pueda deducir que han existido terceros que hayan accedido, descargado o copiado datos sin autorización. Además, se contrató a personal externo a fin de investigar si las contraseñas habían sido compartidas o reveladas a terceras personas, no teniendo razones para pensar que los archivos afectados hubieran sido filtrados al exterior de los sistemas de la sociedad atacada.

Aunque TWITTER en el momento de la apertura de una cuenta no requiere que las personas inserten o introduzcan cual es su país de residencia, resulta evidente que millones de españoles utilizan la citada red social como medio de comunicación; no obstante, de las investigaciones realizadas no puede determinarse el número de contraseñas de usuarios españoles que pudieran haber estado afectados.

De la misma forma, no se tiene constancia de que existan afectados, ni denuncias registradas en la AEPD, ni revelación de datos personales, ni de terceros que hayan obtenido partido o beneficio de la posible quiebra o vulnerabilidad en la seguridad de la red social.

Además, remitido requerimiento de información a la entidad sobre la información publicada y de la posible quiebra esta respondió de manera inmediata a dicha solicitud.

A este respecto, la Sentencia de la Audiencia Nacional de 25/06/2015 ha señalado lo siguiente: *"En interpretación del citado artículo 9, esta Sala ha señalado en múltiples sentencias, (SSAN, Sec. 1ª, de 13 de junio de 2002, Rec. 1517/2001; 7 de febrero de 2003 Rec. 1182/2001; 25-1-2006 Rec. 227/2004; 28 de junio de 2006 Rec. 290/2004 etc), que la obligación que dimana del mismo no se cumple con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca el precepto, y por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva. Hemos considerado, en consecuencia, que se impone una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. En definitiva, toda responsable de un fichero (o encargada de tratamiento) es, por disposición legal, una deudora de seguridad en materia de datos debiendo asegurarse de que dichas medidas o mecanismos se implementen de manera efectiva en la práctica".*

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 **TWITTER SPAIN, S.L** 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