Expediente Nº: E/01903/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **VODAFONE ESPAÑA SAU** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 16 de febrero de 2017, tuvo entrada en esta Agencia escrito de ***VODAFONE ESPAÑA SAU1*** en el que comunican una quiebra de seguridad ocurrida en la denominada base de datos Cellebrite en fecha 06/02/2017 que ha dado lugar a que terceros hayan tenido acceso a datos de correo electrónico y número de teléfono de ciertos clientes.

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:

1.1. CELLEBRITE es una entidad con sede en Israel que tiene suscrito un contrato de prestación de servicio con el GRUPO VODAFONE a nivel mundial con la finalidad de proporcionar una plataforma de diagnóstico para terminales de la compañía que puedan estar sufriendo una avería.

Para realizar las pruebas, las tiendas de Vodafone, tienen instaladas una aplicación web y, por su parte, los terminales que se van a probar deben descargar una aplicación.

Seguidamente se sincronizan ambas aplicaciones por medio de dos códigos, uno que se genera en la aplicación web y se introduce en el terminal y otro que se genera en el terminal y se introduce en la aplicación web.

Seguidamente se realizan una serie de pruebas y se elabora un informe con los resultados. Este informe puede ser impreso o enviado por correo electrónico al cliente.

En este último caso se recoge la dirección de correo y se conserva en la base de datos de Cellebrite junto con el número de teléfono (MSDIN) y el IMEI del terminal.

Toda esta información (informe, MSDIN, IMEI y correo electrónico) se conservan en una base de datos de Cellebrite ubicada en Amazon.

1.2 En fecha 26 de enero de 2017 Cellebrite reportó una brecha de seguridad

sobre la base de datos residente en Amazón, motivada por un acceso por terceros.

El volumen de información comprometido es de 46 GB.

En esta fecha un equipo del Grupo Vodafone se trasladó a la sede de Cellebrite en Israel al objeto de analizar qué información había sido comprometida, detectándose que podría incluir direcciones de correo electrónico y números de teléfono de los terminales analizados de clientes de Vodafone España.

En fecha 27 de enero de 2017 desde Vodafone España se solicita a Cellebrite que deje de recoger información y que proceda al borrado de los datos de los clientes de la entidad, se revisa qué datos pueden no ser necesarios y se decide no recabar el MSDIN. Se revisan determinadas clausulas para reforzar la seguridad.

En fecha 3 de febrero de 2017 se recibe información relativa a los clientes afectados de Vodafone España.

Cellebrite se compromete a realizar el borrado de las bases de datos en fecha 6 de febrero de 2017.

En fecha 5 de febrero de 2017 se bloquea la aplicación.

En fecha 6 de febrero de 2017 Cellebrite aporta un certificado de borrado de las bases de datos.

1.3 Se analiza la información comprometida y se concluye que se ha podido tener acceso a 543 correos electrónicos de clientes que puede considerarse dato personal ya que contienen partes de nombres y apellidos.

En fecha 20 de febrero de 2017 se envía un correo electrónico a los 543 clientes afectados informando de la brecha de seguridad.

Desde el Departamento de Seguridad de la Información de Vodafone España se ha estado rastreando redes sociales y páginas de Internet manifestando en la presente inspección que hasta la fecha no consta que los datos comprometidos hayan sido utilizados por terceros ni indexados por buscadores.

La aplicación de diagnóstico de terminales ha estado desactivada entre las fechas 5 a 28 de febrero de 2017.

2. Los inspectores de la Agencia solicitan acceso al registro de incidencias de la entidad recabando impresiones de pantalla de las relacionadas con la brecha de seguridad sobre la aplicación Cellebrite en el que figura el informe remitido a la Agencia.

3. Aportan copia del contrato de tratamiento entre Vodafone Procurement Company SARL y Cellebrite Mobile Syinchronization Ltd como encargado del tratamiento.

En este contrato se especifica las medidas de seguridad a implementar por el encargado del tratamiento y que la subcontratación de otros encargados del tratamiento se debe realizar previa notificación al responsable del fichero.

4. Aportan informe del Grupo Vodafone en el que se indica que se desconoce el autor

del ataque pero se sospecha de un periodista adversario de Cellebrite. La motivación del ataque era dañar la reputación de Cellebrite no amenazar a Vodafone.

En España consta que hay un total de 550 afectados.

El atacante consiguió acceso al host de backup en la nube de Amazon por medio de una autenticación de usuario robada, supuestamente por phishing, aunque no está confirmado. El acceso se realizó una única vez en la que el atacante copió el back up a un almacenamiento local.

A raíz de este incidente se han realizado las siguientes actuaciones:

a) Asegurarse que los back up no se almacenan en nube nunca más
b) Asegurarse que se adoptan las medidas de seguridad apropiadas
c) Realizar una auditoría al servicio.

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 9 de la LOPD establece:

"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."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

El sistema de información de CELLEBRITE disponía de las medidas de

seguridad establecidas en el Reglamento de desarrollo de la LOPD. Esas medidas incluían las de control de acceso e identificación de usuario, mediante una clave de usuario y contraseña en el caso de ficheros automatizados; y las de gestión de soportes.

En el presente caso, de la información aportada se deduce que el sistema de información (*host de backup en la nube prestado por Amazon*) dónde se almacenaba la base de datos que generaba CELLEBRITE, derivada del servicio que presta a VODAFONE (diagnóstico para terminales de la compañía) , sufrió un ataque indebido y deliberado, que permitió el acceso por medio de una autenticación de usuario robada a información de clientes de VODAFONE ESPAÑA como cuentas de correo electrónico y números de teléfono.

En España consta que hay un total de 550 afectados, sin embargo no consta que los datos comprometidos hayan sido utilizados por terceros ni indexados por buscadores en internet.

Asimismo éstos fueron notificados de la brecha de seguridad tal como prevé el **art 41.3 de la Ley General de Telecomunicaciones** al señalar que:

3. En caso de violación de los datos personales, el operador de servicios de comunicaciones electrónicas disponibles al público notificará sin dilaciones indebidas dicha violación a la Agencia Española de Protección de Datos. Si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas. (…) En la notificación al abonado o al particular se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación. En la notificación a la Agencia Española de Protección de Datos se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales.(…)

Por su parte el **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** (RGPD en adelante), de plena aplicación en fecha de 25 de mayo de 2018, establece en sus artículos 33 y 34 lo siguiente:

C.C.C. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del

tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

***ARTÍCULO 34** Comunicación de una violación de la seguridad de los datos personales al interesado*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

III

El acceso indebido no ha sido consecuencia de las vulnerabilidades del sistema de información atacado, ni a causa de una falta de medidas de seguridad adecuadas o en una ineficaz implantación de las mismas, sino que el atacante realizo el ataque a través de una identificación de usuario y contraseña de un tercero, posiblemente adquirida mediante la *técnica de phsising*, no siendo por tanto responsabilidad de las entidades investigadas los hechos sucedidos.

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".

En este caso, no se ha constatado que las entidades hayan incumplido la obligación de adoptar de manera efectiva las medidas dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros, por lo que no cabe entender infringido el artículo 9 de la LOPD citado.

Procede tener en consideración la Sentencia de la **Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25 de febrero de 2010** que, en relación con un caso similar al presente, señaló lo siguiente:

"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por el ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www..., descargándose una copia de la misma. Y tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.

El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito del derecho administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1999, de 19 de diciembre (RTC 1991/246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de xxx".

No obstante, aunque en la Sentencia no se considera probada una vulneración del artículo 9 de la LOPD, sí se apreció una conducta infractora por parte del responsable del fichero, en concreto la vulneración del deber de guardar secreto, considerando la tardanza de la entidad responsable en adoptar un comportamiento activo para impedir que se hicieran públicos en internet los datos personales comprometidos.

En el presente caso, resulta destacable la diligencia observada por parte de VODAFONE tras detectarse el acceso indebido a la información para minimizar los riesgos y asegurar sus sistemas y comunicar a los afectados la quiebra de seguridad.

IV

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."

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

SE ACUERDA:

PRIMERO.- PROCEDER AL ARCHIVO de las presentes actuaciones.
SEGUNDO.- NOTIFICAR la presente Resolución a **VODAFONE ESPAÑA SAU.**

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