Expediente Nº: E/04157/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante las entidades APPLE MARKETING IBERIA, S.A., y TEABLA COMUNICACIONES, S.L., en virtud de denuncia presentada por Doña ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 11 de junio de 2014, tuvo entrada en esta Agencia un escrito remitido por Doña ***A.A.A.,*** en el que declara lo siguiente:

> Dispone de un Iphone 5S y un Ipad para los cuales ha creado una cuenta en el sistema lCloud de Apple (con ID y contraseña), en la que guarda toda su información: contactos, fotos, aplicaciones, correos, cuenta corriente.
>
> Ha observado que otra persona está metida en su misma cuenta de lCloud y por lo tanto, tiene acceso a toda su información y también ella ve la suya. Entiende que de la misma manera esa persona ve los suyos, por lo que ha tenido una gran pérdida de contactos y de ahí fue donde detectó el problema.
>
> Hace tres semanas, lo puso en conocimiento de Apple, después de seguir sus indicaciones: reseteo de la contraseña de la cuenta Iclod y restaurar de nuevo el iphone, el problema continuó. Le indicaron que era un problema de seguridad y que requería intervención de sus técnicos informáticos para dar solución. Sin embargo no dan solución al problema ni le informan de los trabajos que están realizando.
>
> Considera que es un problema de suma urgencia y gravedad, ya que la cuenta Icloud de Apple, no cuenta con las suficientes medidas de seguridad para garantizar la privacidad de los datos personales.

Junto al escrito de denuncia aporta una impresión de pantalla de los datos relativos a un contacto (nombre y número de teléfono) que manifiesta que pertenece a la agenda de otro usuario, y una fotografía que también manifiesta que está en la nube de otro usuario de Icloud.

Con fecha 10 de julio de 2014 se remite escrito a la denunciante solicitando que aporte la siguiente información y documentación:

> Fechas precisas en la que se produjo el incidente que se describe en la denuncia. Incluya algún tipo de evidencia que pueda confirmar dicha fecha.
>
> Ejemplos y capturas de pantalla en el que se muestren simultáneamente sus datos personales y los datos personales del sujeto que parece compartir su cuenta de I-Cloud.
>
> Número o identificador de incidencia que se le asignó en Apple.

Direcciones, teléfonos y nombres del personal de Apple que atendió su incidencia.

Copia de los correos electrónicos, si los hubo, y de todo registro (en papel u otro) que ha quedado de la tramitación de su incidencia.

Cualquier otra información y evidencia que permita fijar la fecha, la existencia de la brecha de seguridad, el contenido de la incidencia y las respuestas de Apple a la misma.

En respuesta a la solicitud de subsanación remitida a la denunciante, tiene entrada en esta Agencia con fecha 28 de julio de 2014 un escrito de la misma que acompaña copia de los correos remitidos al servicio de APPLE solicitando la cancelación de la cuenta y las respuestas a los mismos y también aporta una impresión de pantalla de la previsión meteorológica en Tanger.

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. La denunciante aporta una impresión de pantalla de los datos relativos a un contacto (nombre y número de teléfono) y una fotografía de lo que parece ser el suelo y unos pies, pero no contiene información de la que se desprenda que dicho contacto pertenezca a una agenda de otro usuario, ni de que esta información estuviese en la nube de APPLE.

   Aporta correos electrónicos de los que se desprende que en junio de 2014 reportó a APPLE una incidencia de seguridad, y que el departamento de ingeniería no pudo solucionarla por lo que acordaron finalmente cancelar la cuenta y abrir una nueva, como consta en el correo electrónico aportado por la denunciante, de fecha 25 de junio de 2014, remitido desde ....@.... al correo de la denunciante.

   La denunciante solicita a APPLE que sean borrados todos los datos de la cuenta.

2. Con fecha 13 de noviembre de 2014 se realizó una visita de inspección en la sede de APPLE MARKETING, IBERIA, S.A., poniéndose de manifiesto los siguientes hechos recogidos así en el Acta de Inspección:

   1. APPLE MARKETING IBERIA SA es filial de APPLE INC en España y en el ámbito nacional es la empresa encargada de prestar servicios de marketing y soporte de ventas a otras empresas del grupo, incluso actuando como comisionista o agente, de toda clase de equipos, productos y sistemas electrónicos y de tecnologías de la información.
   2. APPLE MARKETING IBERIA SA es intermediaria en España de la filial de APPLE en Irlanda APPLE DISTRIBUTION INTERNATIONAL.
   3. En relación con los hechos denunciados, APPLE MARKETING IBERIA SA no dispone de acceso a los sistemas de información de los usuarios de APPLE, si bien los requerimientos realizados por las autoridades españolas son reportadas a un equipo técnico que se encarga de investigarlas y atenderlas en Irlanda.

4. Los inspectores actuantes solicitaron a APPLE MARKETING IBERIA SA como intermediaria en España de la filial de APPLE en Irlanda APPLE DISTRIBUTION INTERNATIONAL, que el plazo de DIEZ días hábiles remitieran a la Agencia Española de Protección de Datos la siguiente información y documentación:

   Confirmación de la existencia de la cuenta con Id de Apple ***C.C.C.*** en las fechas que figuran en los correos electrónicos.

   Relación de accesos a Icloud de dicha cuenta en mayo y junio de 2014, indicando la Id de los usuarios que han realizado dichos accesos.

   Toda la información de las actuaciones realizadas en respuesta a la reclamación efectuada por la usuaria ***C.C.C.*** (Nº de incidencia ***NÚMERO.1).

   Toda la información y documentación que pudieran aclarar los hechos denunciados.

3. Con fecha 24 de noviembre de 2014 tiene entrada en la Agencia Española de Protección de Datos el escrito de respuesta al requerimiento de información realizado en la citada Acta de Inspección, en el que el representante de APPLE DISTRIBUTION INTERNATIONAL manifiesta:

   Investigado este caso específico adjuntan sus notas internas obtenidas del sistema de gestión de clientes. No pueden proporcionar el resto de la información solicitada, dado que la denunciante solicitó la eliminación de su cuenta. En consecuencia han procesado su solicitud de eliminación de la cuenta Apple ID - ***B.B.B.***- con efectos desde el 25 de junio de 2014. La información incluida en sus notas internas sobre el caso son la única información relevante que pueden facilitar.

   Del examen de dichas notas concluyen que los problemas padecidos por la usuaria fueron debidos probablemente a la pérdida de su teléfono original al remitirlo para su servicio técnico en una tienda Movistar. A ella se le hizo entrega de un nuevo teléfono por parte de Movistar. Tras el cambio de terminal, han seguido prestando asistencia a la usuaria y que una vez que solicitó la eliminación de la cuenta señalada anteriormente, terminó la posibilidad de prestar ulteriores servicios en relación con dicha cuenta.

4. Con fecha 23 de abril de 2015 se realizó una visita de inspección en la sede de TEABLA COMUNICACIONES, S.L., en adelante TEABLA, poniéndose de manifiesto los siguientes hechos recogidos en el Acta de Inspección:

   1. TEABLA tiene como objeto social la compra, venta, exportación e importación de productos y servicios de telecomunicaciones, y tiene suscrito un contrato de distribuidor exclusivo con MOVISTAR. Cuenta con una red de 120 tiendas distribuidas en todo el territorio nacional. La tienda que TEABLA disponía en La Moraleja Green fue cerrada en septiembre de 2014 y toda la documentación física de la misma se custodia en el almacén central de la empresa.
   2. TEABLA, como distribuidor oficial de MOVISTAR, dispone de un procedimiento escrito establecido por ésta para la gestión del servicio de

postventa que incluye la gestión del envío al servicio técnico de los terminales móviles entregados por los clientes de MOVISTAR para su reparación.

El procedimiento exige que el cliente que deja su terminal para reparar, firme un acuse de recibo de entrega, en el que se refleja los datos identificativos del cliente y del terminal e incluye las condiciones del servicio. Dicho acuse de recibo se emite por triplicado, quedando una de las copias en poder de TEABLA, otra en poder del cliente y la tercera se envía a MOVISTAR.

El terminal junto con la otra copia del acuse de recibo para movistar firmado por el cliente, es enviado al servicio técnico de MOVISTAR mediante una empresa de mensajería, que en julio de 2014 era la empresa ZELERIS. El mensajero firma un albarán de entrega del terminal que custodia TEABLA.

El servicio técnico de MOVISTAR evalúa el terminal y procede a su reparación o en su caso autoriza la entrega de un terminal nuevo si procede. El terminal reparado, o en su caso, el terminal nuevo se remite por MOVISTAR a la tienda junto con un informe del servicio técnico. Finalmente la tienda entrega el terminal al cliente.

3. Los inspectores actuantes solicitaron al representante de TEABLA que remitiesen en el plazo de dos días a la Agencia Española de Protección de Datos, entre otra documentación, copia de toda la documentación relativa a la gestión de reparación del terminal móvil IPHONE entregado por Dña. ***A.A.A.***, con DNI ***DNI.1, en la tienda de TEABLA sita en La Moraleja Green, incluyendo copia del acuse de recibo firmado por la misma y las condiciones del servicio, copia del albarán de entrega al servicio técnico y copia del albarán de vuelta de dicho servicio.

5. Con fecha 30 de abril de 2015 tiene entrada en la Agencia Española de Protección de Datos un correo electrónico de TEABLA aportando copia del contrato de prestación de servicio de distribución suscrito entre TEABLA y MOVISTAR con fecha 10 de noviembre de 1999, copia del procedimiento de postventa y copia de las condiciones del servicio que se facilita al clientes que entrega el terminal a reparar.

   Respecto a la documentación relativa a la gestión de la reparación del terminal entregado por la denunciante en la tienda de TEABLA de La Moraleja informan que el 23 de abril se solicitó al departamento jurídico de MOVISTAR, donde les informa que están pendientes de recibir la documentación del Servicio Técnico de MOVISTAR.

6. Con fecha 8 de mayo de 2015 tiene entrada en la Agencia Española de Protección de Datos un correo electrónico de TEABLA, en el que su representante manifiesta lo siguiente:

   1. No ha sido posible localizar la documentación en su archivo físico ubicado en Daganzo

   2. Han solicitado reiteradamente a Telefónica información sobre este asunto, sin éxito, si bien finalmente les han dado los siguientes datos, que transcriben literalmente: *"(…) dado que tras la última orden de*

reparación que ahora te remitiremos se informó que el terminal fue extraviado y en base a ello para aportar solución se le hizo una inyección de MOVIS en Por Ser de Movistar"

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 6.1 de la LOPD, señala:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. 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 negocial, 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."

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11 (FJ. 7 primer párrafo)… "*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

En el presente caso, se debe indicar que el hecho de que un tercero acceda a la cuenta creada por la denunciante en el sistema ICloud de Apple (con ID y contraseña), en la que guarda numerosa información, constituye un tratamiento de datos.

III

El Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad sancionadora, establece en el artículo 12, las actuaciones previas, en el sentido siguiente:

"1. Con anterioridad a la iniciación del procedimiento, se podrán realizar actuaciones previas con objeto de determinar con carácter preliminar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

2. Las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia y, en defecto de éstos, por la persona u órgano administrativo que se determine por el órgano competente para la iniciación o resolución del procedimiento".

En el mismo sentido, el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 122 indica:

"1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas".

Las actuaciones previas de investigación se iniciaron como consecuencia de la denuncia presentada en esta Agencia por la denunciante y cuyo contenido se refiere al acceso y tratamiento de sus datos por parte de un tercero incluidos en una cuenta creada en el sistema ICloud de Apple sin que ella lo consintiese.

Con la finalidad de precisar los hechos susceptibles de motivar la incoación del procedimiento, identificar a las personas o entidades que pudieran resultar responsables y las circunstancias relevantes se iniciaron las actuaciones de Investigación, con el

resultado referido en los Hechos de la presente Resolución. Esto es, se requirió información a la entidad responsable de las cuentas ICloud de Apple, así como a la empresa de servicio técnico a la que llevo el terminal móvil para su reparación. No se ha podido averiguar quién es el responsable del problema denunciado, ya que hay varias entidades que han actuado en la cadena de custodia del terminal.

IV

Al Derecho Administrativo sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia. El principio de presunción de inocencia, implica entre otras consecuencias, que corresponde a la Administración acreditar los hechos constitutivos de la infracción

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". De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), establece que "Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que "Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el art. 137 de LRJPAC: *"1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

Por tanto, en el ilícito administrativo no puede prescindirse del elemento subjetivo de la culpabilidad para sustituirlo por un sistema de responsabilidad objetiva o sin culpa» (STS de 12-1-1996 [RJ 1996\156]). «Debe recordarse que, como reiterada doctrina del Tribunal Constitucional y la jurisprudencia de esta Sala, no existe duda de que el principio de culpabilidad y la presunción de inocencia rigen en el ordenamiento sancionador y han de ser respetados en la imposición de cualesquiera sanciones, sean penales, sean administrativas, pues el ejercicio de "ius puniendi" en sus diversas manifestaciones está condicionado por las exigencias constitucionales derivadas de los arts. 24 y 25 de la Norma Fundamental.

En tal sentido, por una parte, no cabe una responsabilidad objetiva y, por otra, 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 corresponde 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.

El derecho a la presunción de inocencia—art. 24.2 CE—prohíbe sancionar sin pruebas, es decir, la imposición de la sanción requiere la previa destrucción de la presunción de inocencia del imputado y ésta sólo se desvirtúa a partir de una prueba de signo incriminador (STS de 3 de mayo de 2004, Sala de lo Militar) que verifique los hechos constitutivos de la infracción y la participación en los mismos del imputado.

En el presente caso, y al hilo de las investigaciones realizadas, se ha acreditado que existió un acceso sin consentimiento a la cuenta en Icloud de la denunciante, y que su teléfono móvil, donde se almacenaban las claves que permitían dicho acceso, fue extraviado sin que conste acreditada la presentación en un establecimiento de servicio técnico en una tienda Movistar. En el presente supuesto, no se ha podido verificar quién ha sido el responsable del error en el control de acceso y en el extravío del terminal de la denunciante, ya que varias entidades habrían actuado, presuntamente, en la cadena de custodia, en el caso de que se hubiera presentado de manera efectiva dicho terminal para su reparación, circunstancia no acreditada; además los datos de la cuenta fueron cancelados tras recibir la petición de la denunciante en ese sentido.

Por tanto, no se pueden imputar el acceso y tratamiento de datos de la denunciante por parte de un tercero al no haber podido acreditar cual es la entidad, en su caso, responsable.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a APPLE MARKETING IBERIA, S.A., a TEABLA COMUNICACIONES, S.L., y a Doña ***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 Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos