



Expediente N°: E/04018/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **EMPLOYEE MOBILITY SOLUTIONS, S.L.** en virtud de denuncia presentada por la misma entidad y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 17/05/2017 tuvo entrada en esta Agencia escrito de **EMPLOYEE MOBILITY SOLUTIONS, S.L.** (en lo sucesivo EMS) en el que pone en conocimiento de este organismo el robo por una persona desconocida de dos ordenadores portátiles que contiene datos de carácter personal de clientes, proveedores, empleados y expedientes para tratamientos de relocalización y expatriación. El robo ha sido realizado en las oficinas de la entidad en MIAMI (EEUU).

Y, entre otra, anexa la siguiente documentación:

Impresión del Incident Report donde figura el robo ocurrido en fecha 24/03/2017.

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 18/09/2017 se solicita información a EMS con objeto de conocer información sobre el robo denunciado y de la respuesta recibida, en fecha 17/10/2017, se desprende:

1. EMS ha aportado denuncia efectuada ante las autoridades de Miami donde se detalla el robo producido y donde la persona que acude informa que:
 - a. No hay señales de entrada forzada a través de la puerta delantera (punto de entrada).
 - b. Hay cámaras de vigilancia en el área alrededor, pero no cerca o en el interior del despacho robado.
 - c. El edificio está abierto para la entrada al público.
2. EMS manifiesta que las oficinas de Miami donde se produjo, se encuentran ubicadas en un edificio compartido con otras empresas y de acceso libre y que un trabajador de la compañía percibió la presencia de terceras personas que supuso que eran personal de mantenimiento o limpieza y posteriormente detectó la falta de dos ordenadores portátiles.
3. EMS manifiesta que los ordenadores están protegidos y el acceso es a través de contraseñas y consideran que es muy difícil el acceso por terceras personas.
4. EMS manifiesta que no tienen constancia de la utilización de los datos contenidos en los portátiles robados.
5. EMS ha aportado Registro de Incidencia de fecha 03/05/2017 donde figura el

robo de los dos portátiles en las oficinas de Miami el día 24/03/2017.

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

El artículo 9.1 de la LOPD establece 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”.

Y el artículo 10, relativo al deber de secreto, establece que:

“El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.”

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.

EMS tiene como objeto social servicios de asesoría migratoria, relocation, mudanza y asesoría fiscal, lo que conlleva el tratamiento de los datos personales relativos a las personas que se relacionan y encargan dichas actividades.

En el presente caso, ha sido la propia entidad la que ha notificado a la Agencia una quiebra de seguridad en sus oficinas de Miami, al serle robados dos ordenadores portátiles, actuando de manera diligente en cuanto tuvo conocimiento de la incidencia producida, registrando la misma, notificándola a la Agencia y denunciando ante las



autoridades competentes norteamericanas el robo perpetrado.

De la información aportada al expediente y de la recabada por los servicios de inspección en fase de actuaciones previas, se desprende que el contenido de la información de los citados dispositivos se hallan totalmente protegida al tener que acceder a la misma a través de contraseñas y sin que se tenga conocimiento que se haya producido su acceso.

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".*

También 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".

En el presente caso, resulta destacable la diligencia observada por parte de la entidad tras detectarse el robo de los ordenadores en sus oficinas registrando la incidencia, notificando la incidencia a la Agencia y denunciando ante las autoridades competentes el robo, sin que hasta la fecha se haya detectado acceso a los datos afectados.

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 **EMPLOYEE MOBILITY SOLUTIONS, S.L.**

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