Expediente Nº: E/05486/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad AMERICAN AIRLINES INC SUCURSAL EN ESPAÑA, en virtud de denuncia presentada por la Dirección General de la Guardia Civil, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 2 de julio de 2014, tuvo entrada en esta Agencia un escrito remitido por la Dirección General de la Guardia Civil en el que se declara lo siguiente:

1. Que agentes de la Guardia Civil de servicio en el Aeropuerto ADOLFO-SUAREZ de Madrid-Barajas han encontrado tres tarjetas de embarque en la puerta R3 del Terminal 4 Satélite de dicho aeropuerto.
2. Las citadas tarjetas, pertenecientes a IBERIA, se encontraban sin ningún tipo de supervisión por parte de empleados de dicha compañía y al alcance de personal ajeno a la misma.
3. Añade la Guardia Civil que en dichas tarjetas, en las que figuran los nombres de sus titulares así como el vuelo y destino, incorporan el sello de "INSPECCIONADO DE SEGURIDAD – AEROPUERTO MADRID BARAJAS", lo que indica que estas personas fueron sometidas a unas medidas adicionales de seguridad por darse en ellas diversas circunstancias de interés.

Junto a la denuncia aporta la siguiente documentación:

Copia de las tres tarjetas de embarque encontradas:

- Tarjeta de embarque con logotipo de IBERIA a nombre de ***A.A.A.***, para el vuelo número ******, de Madrid a Miami del día 5 de junio a las 11:00, sin asiento asignado y operado por AMERICAN AIRLINES. La tarjeta de embarque figura el sello "INSPECCIONADO DE SEGURIDAD– AEROPUERTO MADRID BARAJAS".
- Tarjeta de embarque AMERICAN AIRLINES a nombre de ***B.B.B.***, para el vuelo número ******, de Madrid a Miami del día 5 de junio de 2014 a las 11:00, con asiento 22A y operado por AMERICAN AIRLINES. La tarjeta de embarque figura el sello "INSPECCIONADO DE SEGURIDAD– AEROPUERTO MADRID BARAJAS".
- Tarjeta de embarque AMERICAN AIRLINES a nombre de ***C.C.C.***, para el vuelo número ******, de Madrid a Miami del día 5 de junio de 2014 a las 11:00, con asiento 40G y operado por AMERICAN AIRLINES. La tarjeta de embarque figura el sello "INSPECCIONADO DE SEGURIDAD– AEROPUERTO MADRID BARAJAS".

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. En fecha de 13/3/2015, se realizó una inspección a IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A.U., donde el Gerente de Atención al Cliente de Iberia en el Aeropuerto manifiesta, tras presentarle las tarjetas de embarque objeto de la denuncia, que la operación de embarque asociada al vuelo al que corresponden dichas tarjetas de embarque no fue realizada por personal de IBERIA siendo responsabilidad de la propia AMERICAN AIRLINES.
2. En fecha de 17/4/2015 se realiza una inspección a AMERICAN AIRLINES INC SUCURSAL EN ESPAÑA, (en adelante AA) donde la Coordinadora de Seguridad Internacional de AA, en presencia de una representante la Administración de Seguridad en el Transporte del Ministerio del Interior del Gobierno Americano (Department of Homeland Security) expone ante los hechos de la denuncia lo siguiente:

   2.1. Para los vuelos a EEUU el gobierno de dicho país obliga a controles adicionales que unidos a los controles nacionales llevan a implementar una operativa propia en dichos vuelos que consiste en lo siguiente:

   2.1.1. AA acordona una zona que agrupa a 5 puertas de embarque para cinco vuelos que, con diferentes destinos de EEUU, tienen su salida sobre la misma hora. La zona acordonada es una zona amplía en cuyo interior hay zonas de espera con asientos, tiendas y servicios.

   2.1.2. Existe un primer control para el acceso a la zona acordonada consistente en comprobar la tarjeta y la documentación personal. Este primer control realizado por personal de AA tiene dos finalidades: por un lado dejar pasar a la zona únicamente a los pasajeros que van a tomar alguno de los cinco vuelos, y por otro detectar a los pasajeros que, por exigencia del gobierno de EEUU, deben de pasar por un control adicional implementado dentro de la zona acordonada en una zona habilitada al efecto.

   2.1.3. Para los pasajeros que según el Gobierno de EEUU deben de pasar el control adicional, se les acompaña a la zona habilitada al efecto donde se supervisa el equipaje de mano así como su documentación. La comprobación del equipaje de mano es realizada por personal de una empresa contratada al efecto por AA y tras realizar las comprobaciones incorpora un sello con la leyenda “INSPECCIONADO SEGURIDAD AEROPUERTO MADRID-BARAJAS” a la tarjeta de embarque. A fecha de junio de 2014, esta empresa era VINSA, contratada por AENA, si bien el coste era asumido por AA. Este control es supervisado por personal de Guardia Civil que realiza sobre dichos pasajeros comprobaciones sobre su documentación. Finalizado dicho control, el pasajero queda en libertad de movimiento y con su tarjeta de embarque ya que la necesitará posteriormente, dentro de la zona acordonada, en espera de subir al avión.

   2.1.4. Todos los pasajeros que se encuentran dentro de la zona acordonada deben pasar un último control consistente en leer el código de barras de la tarjeta de embarque como paso previo a subir a su avión. Este control, ubicado junto a cada una de las cinco puertas de embarque es realizado

por personal de AA, que solicita al pasajero la tarjeta de embarque, que es pasada por un lector óptico al objeto de comprobar que dicho pasajero esté en la lista del vuelo correspondiente. Tras esta lectura, la tarjeta es devuelta al pasajero que inmediatamente accede a su avión a través de la puerta de embarque correspondiente.

2.2. En aplicación del Programa Nacional de Seguridad del Ministerio de Fomento existe la obligación para la línea aérea que realiza el procedimiento de embarque de que una vez éste haya finalizado, se recoja toda la documentación que haya podido quedar en las mesas en las que se realiza dicho embarque. Esta obligación implica para AA recoger cualquier documento de viaje incluidas las tarjetas de embarque que pudiera quedar en las mesas en las que se realizan los diferentes controles descritos, no así en las zonas de espera, tiendas y en los servicios que se encuentran dentro de la zona acordonada, zona que se libera una vez han embarcado los cinco vuelos.

2.3. La representante de AA manifiesta que, en ocasiones, algún pasajero pierde la tarjeta de embarque dentro de la zona acordonada. Para estos casos, se puede emitir un duplicado de la tarjeta de embarque en el último control ubicado en la puerta de embarque. De dicha emisión no queda reflejo en el sistema informático de AA.

2.4. Los inspectores muestran a la representante de AA las copias de tres tarjetas de embarque correspondientes al vuelo número ******, de Madrid a Miami del día 5 de junio de 2014 a las 11:00 operado por AA y relativas a ***A.A.A.*** y a ***C.C.C.***, realizándose una búsqueda en sus sistemas informáticos obteniéndose que corresponde a tres pasajeros que efectivamente subieron a dicho vuelo sin que conste en sus sistemas ningún tipo de incidencia sobre dichos pasajeros tal y como consta en el acceso a su sistema informático respecto de dichos pasajeros cuya copia consta en las actuaciones.

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 9 de la LOPD, dispone:

"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."

El art. 9 de la LOPD *establece* el principio de *"seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta a los ficheros el art. 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el "*mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

La entidad AA, en aplicación del Programa Nacional de Seguridad del Ministerio de Fomento, tiene la obligación de que realizado el procedimiento de embarque y una vez éste haya finalizado, se recoja toda la documentación que haya podido quedar en las mesas en las que se realiza dicho embarque. Esta obligación implica para AA recoger cualquier documento de viaje incluidas las tarjetas de embarque que pudiera

quedar en las mesas en las que se realizan los diferentes controles descritos, pero no recoge la documentación que se encuentre en las zonas de espera, tiendas y en los servicios ubicados dentro de la zona acordonada, zona que se libera una vez han embarcado los cinco vuelos.

En consecuencia, tiene incorporadas las medidas de seguridad adecuadas para evitar el acceso por terceros a documentos de los que son responsables.

III

El artículo 10 de la LOPD 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."*

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento.

Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "*El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".*

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "*El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.*

Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la

dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

En el caso que nos ocupa, AA ha explicado detalladamente el procedimiento de embarque para los vuelos que tienen como destino EEUU y las medidas de control especiales establecidas. Las tarjetas encontradas por los agentes de la Guardia Civil de Servicio en el Aeropuerto de Madrid-Barajas, recogieron las tarjetas de tres personas que fueron sometidas a un control especial de equipaje y cuya custodia tenían ellos mismos, que las pudieron dejar olvidadas o pedir un duplicado.

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.

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."*

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."*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de una prueba de cargo acreditativa de los hechos que motivan esta imputación.

En el caso que nos ocupa, no se ha acreditado de forma fehaciente que las tarjetas de embarque encontradas estuviesen custodiadas por AA, por lo que no cabría imputar la responsabilidad de los mismos a dicha aerolínea. Tampoco ha quedado acreditada la responsabilidad de Iberia en los hechos denunciados.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a AMERICAN AIRLINES INC SUCURSAL EN ESPAÑA, y a la Dirección General de la Guardia Civil.

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