Expediente Nº: E/03265/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ASOCIACION HECHOS, en virtud de denuncia presentada por Dirección General de la Policía, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 23 de abril de 2013, tuvo entrada en esta Agencia el oficio número *****/13, del Grupo Número Uno de la Brigada Provincial de Policía Judicial de Burgos, mediante el que se informa del atestado número *****/2013, por si los hechos pudieran constituir incumplimientos a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

En el atestado que adjuntan, ***Don A.A.A.*** denuncia la sustracción de diversos objetos de su vehículo mientras se encontraba ubicado en el Parking E.C. Camino Plata de Burgos. Entre los objetos sustraídos se encuentra un ordenador portátil, queriendo hacer constar ***Don A.A.A.*** que en el disco duro figuran diversos datos de carácter confidencial de menores del Sistema de Protección a la Infancia de Castilla y León y de la Asociación "HECHOS YAKAR", para la cual el denunciante es empleado. También figura en la lista de objetos sustraídos un pasaporte de un menor de edad ***Don B.B.B.,*** de Mali.

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:

- Solicitada información a la Asociación HECHOS YAKAR, sus representantes manifiestan lo siguiente:

"Las actividades realizadas responden a la atención residencial de 4 menores subsaharianos tutelados por la Gerencia de Servicios Sociales de la Junta de Castilla y León y 5 menores tutelados por el Gobierno de Canarias en La Vivienda de Acogida HECHOS-MOOLAADE y HECHOS-YAKAR en Burgos, que se integra en la red de instituciones de Atención a los menores en situación de guarda o tutela. Esta institución se convierte en el núcleo básico y cotidiano de convivencia, siendo muchas las funciones que debe ejercer en el desempeño de su trabajo, teniendo fijadas las siguientes metas:

I. Proporcionar a los menores extranjeros no acompañados un recurso alternativo.

II. Cubrir las necesidades materiales, afectivas y educativas de los menores ingresados.

III. Proporcionar a los niños una formación integral que les permita su integración socio-cultural y laboral.

[…]

Los datos que se intercambian con la Gerencia de Servicios Sociales de la JCYL y el Gobierno de Canarias, son los siguientes:

- *Nombres y apellidos*
- *Nº de Pasaporte*
- *Nº de NIES*
- *Procedencia*
- *Fechas de nacimiento*
- *Informes de proyecto educativo individualizado.*

Los datos que contenía el ordenador sustraído son listados con los nombres y apellidos, NIES, fechas de nacimiento, nº de pasaportes y datos de origen de 65 jóvenes, de los cuales 9 son menores que permanecen bajo nuestra tutela actualmente e información financiera y cuadros estadísticos de la Asociación Hechos.

El ordenador sustraído pertenece a la Asociación Hechos, medio que es utilizado por ***Don A.A.A.*** *para realizar su trabajo como Director General de los Hogares y Pisos Tutelados, para la tramitación de la documentación de los menores ante la Subdelegación de Gobierno y Policía Nacional y obtener la regularización de los mismos. Por tanto* ***Don A.A.A.*** *está autorizado a utilizar la documentación personal de los menores, razón por la cual se encontraba en poder del pasaporte del menor* ***B.B.B.****, ya que se presentó en la subdelegación de Gobierno su documentación para la renovación de su NIE.*

El coche estaba aparcado en el parking del C.C. Camino de la Plata con llave."

Aportan copia de la subvención concedida por la Gerencia de Servicios Sociales de la Junta de Castilla y León y de la Addenda Novena de Adhesión suscrito con el Gobierno de Canarias, para la tutela de menores extranjeros no acompañados.

Consta también en las presentes actuaciones de inspección copia del Documento de Seguridad aplicable a los ficheros de datos personales que maneja la citada Asociación. Del análisis del documento se desprende lo siguiente:

> Se verifica que en el Registro de Incidencias del Anexo VII figura una incidencia, de fecha 13 de abril de 2013 con la descripción "ORDENADOR SUSTRAÍDO DEL COCHE SIMÓN". Como medida correctora figura: "DENUNCIA POLICIA".
>
> En el apartado "4. FUNCIONES Y OBLIGACIONES DEL PERSONAL" figura "*cuando un usuario trate soportes o documentos con datos de carácter personal deberá vigilar y controlar que personas no autorizadas no puedan acceder al soporte físico o documentos por el custodiados".*
>
> El fichero denominado "Fichero de Acción Social y Cooperación Internacional" se encuentra declarado como de nivel Alto. El responsable de Seguridad es ***Don A.A.A.*** junto con una tercera persona. Su acceso al fichero está perfilado como usuario administrador.
>
> El documento de seguridad incluye en su ANEXO V una política de seguridad que establece, entre otros aspectos, las obligaciones de los usuarios, y en su punto 5.3.4 apartado A se cita *"…debiendo evitar la posible salida incontrolada de información de las instalaciones de ASOCIACION HECHOS. No obstante, en supuestos que por motivos justificados de trabajo se requiera la salida de este tipo de soportes de las instalaciones de ASOCIACION HECHOS, se deberá comunicar esta circunstancia al Responsable de Seguridad"*

En el punto 5.3.4.2 se cita "*A. Terminales de trabajo y portátiles. Cada usuario será responsable de su puesto o terminal de trabajo… Respecto de los ordenadores portátiles, deberán mantenerse siempre controlados, evitando su posible sustracción."*

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

Debe valorarse si en los hechos denunciados se ha producido una vulneración de las medidas de seguridad. El artículo 9 de la LOPD, que establece la seguridad de

los datos, 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 citado artículo 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 aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, la pérdida de los datos.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la conservación 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 refiere 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.

Partiendo de tales premisas, deben analizarse a continuación las previsiones que el Real Decreto El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el "Soporte" como el *"objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos".*

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma.

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, concreta las medidas de seguridad. En su artículo 90 indica:

"Deberá existir un procedimiento de notificación y gestión de las incidencias que

afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas."

El artículo 91 del mismo Real Decreto determina lo siguiente:

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Asimismo, en el artículo 92, referido a la Gestión de soportes y documentos se establece lo siguiente:

"1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.

5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que

dificulten la identificación para el resto de personas".

El artículo siguiente establece que el responsable del fichero o tratamiento debe adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

En el supuesto presente, el responsable de la propia Asociación denunció el robo del ordenador que contenía datos personales; asimismo, notificó y documentó la incidencia sucedida el día 13 de abril de 2013, describiéndola detalladamente y adoptando medidas correctoras. En el documento de seguridad consta la autorización del Sr. ***A.A.A.*** para poder sacar de los locales del centro de trabajo el ordenador portátil, así como el perfil de accesos a datos que mantiene, que concuerda con los datos incluidos en el disco duro del ordenador robado.

III

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal en su artículo 10, 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".*

Dado el contenido del citado artículo 10 de la LOPD, 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.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más 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 Constitución Española. En efecto, este precepto en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11, 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"*. *"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" 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."*

El deber de secreto profesional que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda 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 o, en su caso, con el responsable del mismo".* Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la protección de datos a que se refiere la citada Sentencia del Tribunal Constitucional 292/2000, y por lo que ahora

interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

El caso analizado, plantea si concurre una infracción la normativa de protección de datos y el deber de secreto, cuestión que lleva a analizar las siguientes circunstancias que concurren en los hechos denunciados:

Los hechos denunciados se refieren al robo de un ordenador en cuyo disco duro existen datos personales. Para acceder a esos datos existe una clave y contraseña. No se tiene constancia de que dichos datos hayan sido extraídos o accedidos por nadie. Los hechos fueron denunciados de forma inmediata y documentados como exigen las medidas de seguridad referidas en el fundamento anterior; no apreciándose vulneración de la normativa de protección de datos..

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 la Asociación Hechos, a Don ***A.A.A.*** y a la Dirección General de la Policía.

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