



Expediente Nº: E/04586/2011

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad Telefónica Investigación y Desarrollo, S.A., en virtud de denuncia presentada ante la misma por la Policía Municipal de Madrid, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 28 de septiembre de 2011, tuvo entrada en esta Agencia un escrito remitido por la Policía Municipal de Madrid, en el que traslada un informe relativo al hallazgo de documentos con datos personales en escombrera ilegal en el que se dice:

*<<... el pasado día 16 de los corrientes cuando inspeccionaba una zona habitual de vertidos ilegales de escombros, en las inmediaciones de la M-214, encontraron entre otros muchos papeles de un vertido reciente, un dossier, el cual se incluye en el sobre adjunto, conteniendo datos de carácter personal de unas 104 personas pertenecientes al edificio ***EDIF.1 de la calle (C/.....1) de Madrid, ahora en proceso de remodelación total..>>*

Junto al informe, la policía municipal aporta el mencionado documento. Dicho documento denominado “GesPark Gestión de plazas de aparcamiento”, y subtítulo “Datos sobre Asignación de Plazas Edificio ***EDIF.1 – c/ (C/.....1) (MADRID)” consta de 27 páginas, figurando en cada una de ellas datos personales sobre cinco personas. Los datos personales recogidos se corresponden a la fotografía, el nombre, número de teléfono interno, así como las matriculas marca y modelo de vehículos atribuidos a cada uno de ellos, con hasta dos vehículos por persona. El documento aparece en muy mal estado y muestra fecha de confección del 30 de marzo de 2005.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Los representantes de Telefónica Investigación y Desarrollo, S.A., realizan las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:
 - a. La entidad dispone de una normativa corporativa de seguridad de la información, donde se desarrollan las directrices marcadas en la política corporativa de seguridad de la información.
 - b. Igualmente disponen de un procedimiento de seguridad de la información clasificada, dentro de la cual se incluye la información de carácter personal.



c. Para la destrucción de la documentación, ya sea en papel o en soporte informático, existen ubicados en las instalaciones de la compañía una serie de contenedores metálicos cerrados, que periódicamente son retirados por una empresa de destrucción documental que realiza la destrucción física del contenido de los contenedores. Tras su destrucción emite el correspondiente certificado. La gestión de la destrucción de la documentación actualmente la realiza la entidad T-Gestiona, como parte del contrato de arrendamiento de servicios de los edificios en los que se aloja Telefónica.

d. Durante años, la entidad Telefónica Investigación y Desarrollo, S.A., ha mantenido oficinas en la calle (C/.....2) de Madrid, en tanto que el (C/.....1) de esa calle se encontraba ocupado por personal de Telefónica de España, S.A. El complejo de ambos edificios tenía una entrada única, controlada por una empresa de seguridad.

El edificio de la calle (C/.....2) estuvo ocupado hasta el mes de octubre de 2010, fecha en la que finalizó la evacuación del mismo; quedando, únicamente, personal de seguridad, limpieza y un pequeño grupo de personal de Infraestructuras que se dedicó a la retirada de mobiliario, enseres y documentación. Dentro del edificio no quedó nada, como queda recogido en el acta de entrega del mismo a su propietario.

En fecha 5 de mayo de 2011 se procedió a la entrega del edificio, levantándose la correspondiente acta de devolución.

e. La seguridad del edificio de la calle (C/.....2) estuvo encomendada la entidad SECURIBER, S.L.U. Se recaba copia del contrato con dicha entidad.

f. A fin de controlar los accesos al edificio se entregó al personal de seguridad un documento en el que se relacionaba todo el personal con acceso al parking.

g. Durante el tiempo en que la entidad estuvo ocupando el edificio de (C/.....2), para la destrucción de la documentación la entidad utilizaba los servicios de DATABOX, basándose la relación entre las entidades en la realización de solicitudes y la emisión de facturas.

h. Durante la evacuación del edificio de la calle (C/.....2), se utilizaron los servicios de ***EMPRESA.1, S.L. (en adelante MSO), para la retirada y posterior destrucción de material sobrante, lo que incluía la documentación en papel, sin que existiese contrato específico, si bien en cada remesa destruida se emitió el correspondiente certificado de destrucción.

Aportan copia de trece certificados emitidos a la entidad en el periodo comprendido entre septiembre de 2010 y febrero de 2011.

2. Mostrada la documentación encontrada por la Policía, los representantes de la entidad manifiestan que:

a. Dicho documento es el facilitado por la entidad al personal de seguridad para la realización del control de accesos de vehículos al aparcamiento por personal de la entidad que trabajaba en el edificio de (C/.....2).

b. Dicho documento recoge únicamente personal propio de Telefónica Investigación y Desarrollo, S.A., que tenía autorizado el acceso al parking del edificio.



- c. El documento se generó con la aplicación GESPARK, que se utilizaba para la gestión de las plazas de aparcamiento. Mediante dicha aplicación se realizó la impresión del documento.
- d. A la vista de la fecha del documento, el 30 de marzo de 2005, manifiestan los representantes de la entidad que se trata de un documento base que recogía los usuarios del parking en aquel momento.
- e. Posteriormente al personal de seguridad se le facilitó el acceso a una aplicación informática mediante la cual podían verificar las autorizaciones de acceso al aparcamiento.
- f. La empresa de seguridad tenía la obligación de devolver o destruir la documentación de carácter personal una vez cumplida la prestación contractual, tal como se recoge en el contrato suscrito.
- g. Telefónica solicitó a la empresa de seguridad un certificado de que dicha documentación había sido destruida, si bien nunca se ha recibido dicho certificado.
- h. Entienden los representantes de la entidad que, al haber aparecido el documento encontrado por la Policía y origen de las presentes actuaciones en un vertedero de escombros en septiembre de 2011, el documento debió quedar en la garita de seguridad y que, con motivo de las obras que se están realizando actualmente en el edificio de (C/.....2) por el propietario del mismo, han debido ser arrojados, junto con los escombros originados por dichas obras.
- i. Entienden además que era obligación del propietario del edificio el haber devuelto a Telefónica el documento hallado, en lugar de haberlo arrojado junto con los escombros.

Finalizada la inspección, los inspectores realizaron una visita guiada dentro del edificio, donde los representantes de la entidad mostraron contenedores metálicos tipo buzón, destinados a la recepción de documentación confidencial, tomando una fotografía de uno de ellos.

3. Mediante escritos con entradas en esta Agencia en fechas 20 y 25 de junio de 2012 la entidad inspeccionada aportó la siguiente documentación:
 - Certificado de Shredex Ibérica Empresa de Destrucción confidencial de Documentos S.L. que acredita cómo lleva a cabo T-Gestiona, a través de esta empresa, la recogida y destrucción de la información recogida en los contenedores metálicos mostrados a los inspectores durante la inspección. Aportan varios certificados de gestión documental.
 - En cuanto a la copia del contrato suscrito con la entidad Databox para la destrucción documental, solicitado durante la inspección, informa la entidad que estos servicios se prestaban bajo los pedidos que el Departamento de Compras periódicamente emitía. Aporta varios ejemplos de dichos pedidos, de las facturas emitidas por Databox en la que se describen tanto los equipos alquilados como los servicios facturados y varios ejemplos de los Certificados de destrucción emitidos por Databox.



- Documento denominado “CONDICIONES PARTICULARES PARA LA PRESTACIÓN DEL SERVICIO DE ARCHIVO FÍSICO EXTERNO Y DIGITALIZACIÓN BÁSICA PARA DISTRITO C”.
- Documento denominado “INDICADORES DE NIVEL DE CALIDAD DEL SERVICIO DE ARCHIVO FÍSICO EXTERNO Y DIGITALIZACIÓN BÁSICA PARA DISTRITO C”.

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

La documentación aportada por la Policía Municipal de Madrid se conforma de un documento con datos personales de alrededor de cien trabajadores de Telefónica, que estaban acreditados para entrar en el parking de la entidad; teniendo fecha de 30 de marzo de 2005.

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 concurren 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 Policía Municipal de Madrid, en la que se indicaba que había encontrado en una escombrera ilegal un documento con datos personales, documento que se encuentra en muy mal estado y está fechado el día 30 de marzo de 2005.

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 mencionadas, con el resultado referido en los Hechos de la presente Resolución.

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 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 libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, 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.

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 contiene, en palabras del Tribunal Constitucional en la citada Sentencia 292/2000, un *“instituto de garantía 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 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.

En el caso denunciado, la Policía Municipal de Madrid indicó que había encontrado un documento con datos personales en una escombrera ilegal, documento que se encuentra en muy mal estado y que envió a esta Agencia.

IV

La aplicación de las medidas de seguridad por parte de las empresas que tratan datos de carácter personal es una obligación de gran trascendencia. Aún en el caso de que una empresa se traslade o cese en su actividad, debe decidir que hace con los documentos generados que contienen datos personales, pudiendo bloquearlos o destruirlos en función de que continúen siendo necesarios o pertinentes en relación con las finalidades para las que se recabaron, o mantenerlos por establecerlo las disposiciones legales o las relaciones contractuales. En el supuesto de que no sean destruidos, deben mantenerse las medidas de seguridad exigidas para el tipo de datos que se traten, para evitar, entre otras cosas, que puedan ser depositados en la vía pública al acceso de cualquier persona.

Tras las actuaciones previas de investigación, se ha acreditado que Telefónica tiene las medidas de seguridad exigibles a los documentos en papel. Asimismo, tenía un contrato con una empresa de seguridad para acceder a los edificios de la (C/.....1) y (C/.....2), al tener una entrada única y estar ocupados por dos empresas de Telefónica. En el contrato con la empresa de seguridad tenían pactado que los documentos generados por la aplicación para control del parking serían destruidos o devueltos a Telefónica para su destrucción. Por otro lado, el edificio ha sido entregado a su propietario en el mes de octubre de 2010, quedando vacío como consta en el acta de entrega. Suponen que ese documento quedaría en la garita de seguridad y fue depositado en la escombrera por el propietario del edificio durante las obras que se están efectuando en el mismo.

La documentación aportada por la Policía Municipal de Madrid se refiere, únicamente, a un listado del año 2005, habiendo transcurrido más de 6 años desde que se generó hasta que lo ha encontrado la Policía Municipal en una escombrera ilegal.

El artículo 47 de la LOPD, bajo el epígrafe *“Prescripción”*, establece:

“1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la



infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.”

Los hechos valorados en las presentes actuaciones, relacionados con la posible falta de medidas de seguridad, que han podido dar lugar a un acceso por parte de terceros a los datos de carácter personal contenidos en dos contratos, se remontan al mes de marzo de 2005, habiendo tenido esta Agencia conocimiento de los mismos por virtud de la citada denuncia registrada de entrada en el Organismo en fecha 28 de septiembre de 2011.

Así, considerando que el plazo de prescripción comienza a contarse el día en que se cometió la presunta infracción, en el presente caso el “*dies a quo*” del cómputo prescriptivo debe fijarse en el mes de marzo de 2005, resultando que la posible infracción de la falta de medidas de seguridad, ha prescrito de conformidad con lo dispuesto en el mencionado artículo 47.1 de la LOPD, que establece unos plazos de prescripción de tres años para las infracciones muy graves, dos para las graves y un año para las leves, ya finalizados cuando la denuncia respectiva tuvo entrada en esta Agencia Española de Protección de Datos.

Teniendo en cuenta, además, que de conformidad con lo dispuesto en el apartado 3 del precepto antes citado, así como en el artículo 132.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPCA), el único modo de interrumpir el cómputo del plazo de prescripción es la iniciación, con conocimiento del interesado, del oportuno procedimiento sancionador, y en el presente caso, al no haber tenido conocimiento de los hechos con anterioridad, y al no poder determinar a la persona o entidad presuntamente infractora para aclarar lo sucedido, no ha sido posible formalizar dicha incoación dentro de plazo establecido, procede declarar la prescripción de la presunta infracción con archivo de las actuaciones.

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 Telefónica Investigación y Desarrollo, S.A., y a la Policía Municipal de Madrid.

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.