Expediente Nº: E/02325/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante ***A.A.A.*** en virtud de denuncia presentada por la POLICIA MUNICIPAL DE MADRID y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 16 de marzo de 2017, tuvo entrada en esta Agencia escrito de POLICIA MUNICIPAL DE MADRID en el que denuncia a ***A.A.A.*** como propietario del "Locutorio B.B.B." en el que los clientes acceden a ordenadores donde no se realizan borrado de datos de sesiones anteriores, estando a disposición de los usuarios la información que previamente han dejado los anteriores usuarios que han utilizado los equipos.

Que según la POLICIA MUNICIPAL DE MADRID los hechos tuvieron lugar hasta el 2/3/2017. Y, entre otra, anexa la siguiente documentación:
Tres discos duros intervenidos en los ordenadores de uso público
Fotos de pantalla donde aparecen fotos e historiales de navegación.

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 POLICIA MUNICIPAL DE MADRID, manifiesta en su informe-denuncia que "[…] en el local existen diferentes ordenadores de uso público en el que no se realiza borrado de la información introducida […] *En dichos ordenadores se localizan tanto archivos de imagen, fotografías personales de los clientes, archivos de texto en diferentes formatos, que van desde currículos hasta reportes bancarios, como todo el historial de páginas web y redes sociales visitadas por cada uno de los clientes, en algún caso incluso de años anteriores*".

2. La existencia de datos de carácter personal se desprende de la diligencia de "Datos Extraídos" en la que se extraen distintos ficheros como fotografías a DNI o tarjeta de ciudadanía. También se extraen documentos en los que aparecen número de afiliación de la seguridad social nóminas o certificados bancarios.

3. El que estos datos eran accesibles por diferentes clientes se desprende en que dichos datos residían en las mismas carpetas genéricas, con información de distintas personas y fechas de creación espaciadas en el tiempo. También se puede observar el historial de navegación con fechas de años anteriores.

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 9 de la LOPD establece a cerca de la seguridad de los datos 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.

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, el "acceso no autorizado" por parte de terceros.

La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se refiere a normas reglamentarias.

El Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21de diciembre, (RDLOPD en lo sucesivo) establece un régimen específico de "seguridad" a implantar por el responsable del fichero para salvaguardar la tutela debida a un derecho fundamental ex artículo 18.4 de la Constitución Española, de conformidad con la doctrina sentada por la STC 292/2000.

Derecho que se conculca desde el momento de la inobservancia de tales medidas que devienen en una indefensión de la privacidad de los datos y en un acceso a éstos por parte de terceros que no están legitimados y cuyo uso no es controlable y que encuentra únicamente el límite de su voluntad, lo que va en menoscabo del derecho fundamental a la protección de los datos de carácter personal.

El citado RDLOPD dedica el TÍTULO VIII bajo la rúbrica "*De las medidas de seguridad en el tratamiento de datos de carácter persona*l", en su Capítulo III a establecer el catálogo de medidas de seguridad a aplicar en los ficheros atendiendo a

los distintos niveles de seguridad que se establecen en su artículo 80, ya sean de nivel básico, medio o alto.

Asimismo, en cuanto a la conducta típica, como elemento fundamental para el desarrollo de la potestad sancionadora, nos dice el artículo 44.3 h) de la LOPD, que considera infracción grave "*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*"

Establecido el régimen jurídico aplicable a los hechos denunciados, debe realizarse el análisis de éstos y determinar su encaje normativo, a saber:

Los hechos denunciados consisten en que los clientes del locutorio que utilizaban el servicio de acceso a internet, utilizaban equipos en los que no se realizaba un borrado de la información que dejaban los anteriores usuarios, que hubieran utilizado el mismo equipo, de modo, que cualquier usuario "nuevo" podía acceder a toda la información que *se habían dejado los anteriores*. Información de lo más variada, que va desde documentos personales, como DNI, pasaportes, certificados bancarios, etc., hasta historial de navegación a través de los exploradores de internet de los equipos, dónde se almacenaban las páginas visitadas, pudiéndose encontrar sesiones abiertas en redes sociales, bandejas de entrada de cuentas de correo, etc.

No obstante lo anterior, en los hechos que se denuncian no se ha producido ningún incumplimiento de las medidas de seguridad previstas en el Capítulo III del Título VIII del RLOPD, por lo que no es posible incardinar los hechos sucedidos – la no eliminación de los datos- en el citado catálogo. Lo que impide apreciar la conducta típica y antijurídica que establece el artículo 44.3 h) antes citado, siendo la solución procedente en derecho el archivo de las actuaciones.

III

No obstante lo anterior, debe indicarse que el próximo de 25 de mayo de 2018, será de plena aplicación el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (RGPD en adelante), y que de acuerdo con sus disposiciones, y en relación con las medidas de seguridad basadas en la *evaluación de impacto* y *enfoque del riesgo* que debe realizar el responsable del fichero o tratamiento, éstas deben ser acordes con el tipo de tratamiento que se vaya a realizar, sin que estén previamente tasadas por la norma, sino que se establece la responsabilidad de la entidad a implementar las medidas adecuadas en función del tipo de tratamiento que realice.

Establece el Artículo 32.1 b) del RGPD lo siguiente:

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y

organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (El subrayado es de la Agencia Española de Protección de Datos)

Por su parte, en los considerandos del citado RGPD se establecen previsiones al respecto:

(76) *La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.*

(83*)….Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales….*

(84*)… El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento…*

(90)*…Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento….*

(El subrayado es de la Agencia Española de Protección de Datos)

Por lo expuesto a la fecha de plena vigencia del RGPD, todo responsable del tratamiento deberá implementar las medidas de seguridad **adecuadas al tratamiento que se realice**, medidas que pueden no estar tasadas en la norma y que facilitaran la seguridad, confidencialidad e integridad, de los datos en relación con el tratamiento de datos personales por su concreta y previa determinación.

IV

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."*

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO.- PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO.- NOTIFICAR la presente Resolución a ***A.A.A.*** y POLICIA 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 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