Procedimiento Nº: A/00186/2013

RESOLUCIÓN: R/00101/2014

En el procedimiento A/00186/2013, instruido por la Agencia Española de Protección de Datos a la entidad CENTRAL 238, S.L., vista la denuncia presentada por D. ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 28/08/2013, tuvo entrada en esta Agencia un escrito de D. ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia una posible vulneración de la normativa de protección de datos en el portal web de la compañía "MEX TRANSPORTE URGENTE", en el que pueden visualizarse los datos personales asociados a un número de albarán, incluidos los correspondientes a otros destinatarios, sin más que introducir cualquier número al azar.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se tuvo conocimiento de los siguientes extremos, que constan detallados en el Informe de Actuaciones Previas elaborado:

1. En fecha 10 de septiembre de 2013 por la Inspección de Datos se ha verificado que, al introducir el número de albarán indicado por el denunciante (de 12 dígitos) en la casilla correspondiente de la página principal del sitio web https://mex.es (*Consulta tu envío*), se accede a los datos del envío en cuestión, incluyendo el nombre y apellidos del denunciante, el domicilio completo de entrega del envío, número de teléfono y dirección electrónica. Se indica asimismo la fecha de entrega (28/8/2013) y el número del DNI del receptor.
2. En la misma fecha se ha verificado que, al modificar el último dígito del citado número de albarán, puede accederse sucesivamente, sin ningún tipo de restricción, a los datos asociados a los correspondientes albaranes de envío.
3. Según la información proporcionada por RED.ES a través de www.nic.es, el dominio *MEX.ES* es titularidad de la compañía CENTRAL 238, S.L. (en lo sucesivo CENTRAL 238).

TERCERO: Con fecha 30/09/2013, el Director de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 45.6 de la LOPD, acordó someter a la entidad CENTRAL 238 a trámite de audiencia previa al apercibimiento, en relación con la denuncia por infracción del artículo 9 de la LOPD, en relación con los artículos 91 y 93 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la citada Ley Orgánica, tipificada como grave en el artículo 44.3.h) de la misma norma.

Con tal motivo, se concedió a la entidad CENTRAL 238 plazo para formular alegaciones, que transcurre sin que se haya recibido escrito alguna en esta agencia Española de Protección de Datos.

HECHOS PROBADOS

PRIMERO: La entidad CENTRAL 238 es titular del dominio web *MEX.ES*.

SEGUNDO: Con fecha 10/09/2013, por los Servicios de Inspección de la Agencia Española de Protección de Datos se verifica que, al introducir el número de albarán de doce dígitos indicado por el denunciante (destinatario del envío) en la casilla correspondiente de la página principal del sitio web https://mex.es (*Consulta tu envío*), se accede a los datos del envío en cuestión, incluyendo el nombre y apellidos del mismo, el domicilio completo de entrega del envío, número de teléfono y dirección electrónica. Se indica asimismo la fecha de entrega (28/08/2013) y el número del DNI del receptor.

Asimismo, se constata que, al modificar el último dígito del citado número de albarán, puede accederse sucesivamente, sin ningún tipo de restricción, a los datos asociados a los correspondientes albaranes de envío.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

El Titulo VII sobre *Infracciones y sanciones*, el artículo 43 de la LOPD establece:

"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."

III

Se imputa a la entidad CENTRAL 238 el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros.

El Art. 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"Seguridad de los datos:
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

El Art 17.1 de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:
1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar

las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD, traspuso al ordenamiento interno el contenido de la Directiva 95/46. En el artículo 9 de la citada LOPD se dispone lo siguiente:

"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 la 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 trascrito 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 dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

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 al concepto de "*fichero*" el artículo 3.b) de la LOPD lo define como *"todo conjunto organizado de datos de carácter personal",* con independencia de la modalidad de acceso al mismo.

Por su parte el artículo 3.c) de la citada Ley Orgánica considera tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente procedimiento, la *"comunicación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados o no.

Por su parte, el artículo 3.a) de dicha Ley añade que se entenderá por datos de carácter personal *"cualquier información concerniente a personas físicas identificadas o identificables".* En este mismo sentido se pronuncia el artículo 2 a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos profesionales y a la libre circulación de estos datos, que dispone *"toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".*

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...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.

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. Dichas medidas, en el caso que nos ocupa, deben salvaguardar la confidencialidad y seguridad de los datos de carácter personal recabados por CENTRAL 238 de los destinatarios de los envíos que le son encargados por sus clientes, correspondiendo adoptar las calificadas de nivel básico, en atención al tipo de información que contiene, tal como se especifica en el art. 80 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD. El artículo 81.1 del citado Reglamento señala que *"Todos los ficheros o tratamiento de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico"*.

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104, del Reglamento de desarrollo de la LOPD.

Los artículos 91 y 93 del citado Reglamento, aplicable a todos los ficheros y tratamientos automatizados, establecen:

"Artículo 91. Control de acceso.

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".

Este artículo desarrolla las previsiones que deberá establecer el responsable del fichero para garantizar que los usuarios con acceso a datos personales o recursos, por haber sido previamente autorizados, sólo puedan acceder a tales datos y recursos. Para ello es necesario que se implanten mecanismos de control para evitar que un usuario pueda acceder a datos o funcionalidades que no se correspondan con el tipo de acceso autorizado para el mismo, en función del perfil de usuario asignado.

"Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible".

El artículo 5.2.b) del citado Reglamento define la autenticación como el procedimiento de comprobación de la identidad de un usuario; y el mismo artículo, letra h), se refiere a la identificación como el procedimiento de reconocimiento de la identidad de un usuario. Corresponde al responsable del fichero o tratamiento comprobar la existencia de la autorización exigida en el citado artículo 91, con un proceso de verificación de la identidad de la persona (autenticación) implantando un mecanismo que permita acceder a datos o recursos en función de la identificación ya autenticada. Cada identidad personal deberá estar asociada con un perfil de seguridad, roles y permisos concedidos por el responsable del fichero o tratamiento.

En definitiva, la entidad CENTRAL 238 está obligada a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

En este caso, los hechos expuestos, en relación con la posibilidad de que por parte de terceros se pudiera acceder, a través de Internet, a los datos personales contenidos en la base de datos de CENTRAL 238, sin haber garantizado la seguridad de tales datos de carácter personal, suponen la comisión, por parte de dicha entidad, de una infracción del artículo 9.1 de la LOPD, al haberse constatado que a través del sitio web https://mex.es, cuya titularidad corresponde a la citada entidad, en el apartado habilitado por la misma para que los clientes puedan realizar el seguimiento de sus envíos (*Consulta tu envío*), se puede acceder a la información asociada a los albaranes en cuestión, con el detalle de los datos personales de los destinatarios respectivos (nombre y apellidos del denunciante, el domicilio completo de entrega del envío, número de teléfono y dirección electrónica), así como el DNI. Concretamente, los Servicios de Inspección de la Agencia constataron que, al introducir el número de albarán

indicado por el denunciante (de 12 dígitos) en la casilla correspondiente de la página principal del sitio web https://mex.es (*Consulta tu envío*), se accede a los datos del envío, y que modificando el último dígito del citado número de albarán puede accederse sucesivamente, sin ningún tipo de restricción, a los datos asociados a los mismos, sin que se observase control de acceso alguno.

Así, los datos personales de los receptores de los envíos encargados a CENTRAL 238 por sus clientes resultan accesibles a terceros, siendo ello consecuencia de una insuficiente o ineficaz implementación de las medidas de seguridad detalladas. Dado que ha existido vulneración del *"principio de seguridad de los datos"*, se considera que el CENTRAL 238 ha incurrido en la infracción grave descrita.

En esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

IV

El artículo 44.3.h) de la LOPD, 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".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que CENTRAL 238 ha incurrido en la infracción grave descrita.

V

El apartado 6 del artículo 45 de la LOPD establece lo siguiente:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho

incumplimiento".

A este respecto, procede considerar lo establecido en el artículo 45.4 y 5 de la LOPD, que establece lo siguiente:

"4. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
a) El carácter continuado de la infracción.
b) El volumen de los tratamientos efectuados.
c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
d) El volumen de negocio o actividad del infractor.
e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
f) El grado de intencionalidad.
g) La reincidencia por comisión de infracciones de la misma naturaleza.
h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas.
i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.
j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:
a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.
b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.
c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.
d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.
e) Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado artículo 45.6 de la LOPD. Junto a ello se constata una cualificada disminución de la culpabilidad de la entidad denunciada por la concurrencia de varios criterios de los enunciados en el artículo 45.4 de la LOPD, concretamente, el grado de intencionalidad apreciado y que no constan beneficios obtenidos como consecuencia de la comisión de la presunta infracción y que no consta vinculación de la actividad de CENTRAL 238 con la realización de tratamientos de datos de carácter personal.

La entidad CENTRAL 238 deberá adoptar medidas correctoras para impedir el acceso indiscriminado a los datos personales registrados en sus sistemas de información, mostrando en el apartado habilitado en su web para el seguimiento de los envíos únicamente el estado de los mismos, evitando que resulten visibles por esta vía los datos de carácter personal.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00186/2013**) a la entidad CENTRAL 238, S.L. con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en relación con la denuncia por la infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica, respectivamente, y de conformidad con lo establecido en los artículos 36 y 37.a), f) y n) de la LOPD, que atribuye la competencia **al Director de la Agencia Española de Protección de Datos.**

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- REQUERIR a CENTRAL 238, S.L., de acuerdo con lo establecido en el apartado 6 del artículo 45 de la Ley 15/1999, para que en el plazo de un mes desde este acto de notificación:

2.1.- CUMPLA lo previsto en el artículo **9** de la LOPD. En concreto se insta al denunciado a adoptar, de manera efectiva, las medidas técnicas y organizativas que garanticen la seguridad de los datos personales, que impidan el acceso indiscriminado y sin restricciones por parte de terceros a los datos personales registrados en sus sistemas de información, y sin el consentimiento de los afectados, estableciendo mecanismos para que la información resulte accesible únicamente a los interesados, o bien mostrando en el apartado habilitado en su web para el seguimiento de los envíos únicamente el estado de los mismos, evitando que resulten visibles por esta vía los datos de carácter personal.

2.2.- INFORME a la Agencia Española de Protección de Datos del cumplimiento de lo requerido en el apartado anterior, aportando aquellos documentos en los que se ponga de manifiesto dicho cumplimiento.

Se le advierte que en caso de no atender el citado requerimiento, para cuya comprobación se abre el expediente de investigación **E/00370/2014**, podría incurrir en una infracción del artículo 37.1.f) de la LOPD, que señala que "*son funciones de la Agencia de Protección de Datos: f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones."*, tipificada como grave en el artículo 44.3.i) de dicha norma, que considera como tal, *"No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma",* pudiendo ser sancionada con multa de **40.001 € a 300.000 €,** de acuerdo con el artículo 45.2 de la citada Ley Orgánica.

3.- NOTIFICAR el presente Acuerdo a la entidad CENTRAL 238, S.L.

4.- NOTIFICAR el presente Acuerdo a D. ***A.A.A.***.

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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos