Expediente Nº: E/00261/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad GENERAL LOGISTICS SYSTEMS SPAIN, S.A. (con anterioridad AGENCIA DE SERVICIOS DE MENSAJERIA, S.A.,), en virtud de la denuncia presentada por ***D. B.B.B.*** y teniendo como base los siguientes

HECHOS

PRIMERO: GENERAL LOGISTICS SYSTEMS SPAIN, S.A. (en lo sucesivo GLSS), el 12/12/2017 informó a la Agencia que había sufrido un incidente de seguridad en su Sitio Web. Un usuario ha accedido a determinados datos y documentos de producción de GLSS sin la autorización preceptiva para hacerlo, exigiéndonos una suma de dinero con la amenaza de hacerlo público.

Que con carácter inmediato la empresa ha puesto en marcha un protocolo de seguridad para restringir dicho acceso única y exclusivamente a los titulares de datos y al personal autorizado a la gestión de los mismos.

Que además están realizando una Auditoría externa especializada en la detección de posibles ataques o vulnerabilidades de nuestro Sitio Web, con el objetivo de esclarecer los hechos y evitar que un incidente similar pueda ser producido en modo alguno.

Que una vez conocido dicho incidente y con carácter inmediato, la empresa puso en marcha un protocolo de seguridad para restringir dicho acceso y resolvió el incidente.

Que en la misma fecha se ordenó una auditoría externa especializada que detectó que el usuario accedió a un total de 28 albaranes de entrega que incluyen datos personales de otros usuarios.

Que con fecha 02/01/2018, no habiendo pagado al usuario cantidad alguna, ha remitido comunicaciones a los principales clientes (empresas FNAC, Amazon,.. GLS, IPC) y nuevamente a GLSS, reclamando una suma igual a 300.000 euros por un supuesto daño moral. En el mismo escrito exige este usuario que se le comuniquen las empresas que habrían proporcionado sus datos, que se borren sus datos de nuestros ficheros y se guarden en un expediente seguro para aportar en juicio llegado el caso, así como que se le sea remitido un informe detallado y completo de cómo se han tratado dichos datos por nuestra empresa.

Esta información dio lugar a la apertura del expediente de actuaciones previas E/00261/2018.

SEGUNDO: Con fecha 02/01/2018 tuvo entrada en esta Agencia escrito de B.B.B. (en lo sucesivo el denunciante), en el que denuncia a ***GENERAL LOGISTICS SYSTEMS SPAIN, S.A.*** (en lo sucesivo GLSS, con anterioridad AGENCIA DE SERVICIOS DE MENSAJERIA, S.A.) por los siguientes hechos: que se ha cometido infracción a la LOPD en relación con las medidas de seguridad dejando a expuestos millones de datos personales referidos al nombre y apellidos, domicilio, teléfono, etc, motivado por dejar sin seguridad los albaranes digitalizados de entrega a sus destinatarios cuyos datos eran accesibles desde la web con tan solo cambiar un número de la cifra asignada a los citados albaranes.

La denuncia como la documentación adjunta a la misma y la incorporada como consecuencia de las actuaciones de investigación dió lugar al E/00452/2018.

TERCERO: 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:

Los representantes de GLSS manifiestan:

En relación a las medidas de seguridad adoptadas para acreditar la identidad de un cliente antes de darle acceso a su albarán de entrega y copia del DNI en el año 2017.

Durante 2017, las aplicaciones informáticas en GLS permitían hacer el seguimiento de un envío tanto al cliente que contrata los servicios de transporte como al destinatario del mismo.

El destinatario no podía acceder al albarán de entrega ni a copias del Documento Nacional de Identidad. La aplicación tan solo permitía hacer un seguimiento del envío expresando el estado del mismo.

El cliente podía acceder al albarán de entrega a través de la aplicación previo acceso de USUARIO y CONTRASEÑA.

En diciembre de 2017 se ha modificado el método para generar el código del enlace de la página que permite consultar el albarán. Se utiliza a partir de esta fecha un método conocido como IDENTIFICADOR ÚNICO GLOBAL (en inglés Globally Unique Identifier o GUID) en lugar del código de expedición más el código de plaza de origen que se exigía hasta dicha fecha.

Además, la aplicación de GLS en el caso de clientes personas físicas, ha eliminado el nombre del destinatario siendo sustituido por la expresión genérica PARTICULAR, en lugar del nombre de la persona o del nombre del destinatario que nos hubiera sido facilitado originariamente por el cliente que contrató el transporte con GLS. Estas modificaciones han sido realizadas para incrementar el nivel de seguridad de protección de la información e impedir un acceso a dicha información por parte de personas no autorizadas.

En relación a los motivos por los que un cliente puede acceder a albaranes de terceros tan solo modificando el último número de la URL con varios enlaces como ejemplo.

El enlace no se le proporcionaba en ningún caso al destinatario de un envío. Dicho enlace iba dentro del código fuente de la página del enlace, que se le proporcionaba al cliente para el seguimiento del envío. Por lo que, cuando se diseña originariamente el enlace pareciera suficiente que el nivel de seguridad exigido consistiera en el código de la expedición y el código de plaza.

Los enlaces que permitían acceso a albaranes y DNI se corresponderían a envíos anteriores a un cambio realizado en 2015, a partir del cual ya no era posible acceder a albaranes desde la página de seguimiento del envío y se tenía que disponer del enlace, el cual no era proporcionado a los destinatarios por parte de GLS.

En relación al motivo por el que, sin autenticación de usuarios, se puede acceder a imágenes de Documentos Nacionales de Identidad.

Los enlaces que permiten acceso a DNI son relativos a documentos que se han previsto como justificativos de la entrega de los envíos. En ningún caso han sido diseñados para incluir imágenes de documentos nacionales de identidad ni tampoco

para poner éstos a disposición de ningún destinatario. Dichos enlaces no se facilitan al destinatario de un envió. Tan solo en casos excepcionales se podría dar dicho enlace al cliente si este reclamase de forma expresa la no entrega de un paquete. En dichos supuestos se proporcionarían y serian accesibles por parte del cliente previo acceso con usuario y contraseña, o ser proporcionados ad-hoc y bajo petición a GLS de forma expresa mediante medios electrónicos.

Para poder acceder a las imágenes se debía conocer la existencia del enlace. A partir del enlace se tenía que conocer la fecha de entrega, el código de expedición y el código de la plaza de origen, lo que limitaba sustancialmente su accesibilidad.

Se ha revisado el fichero que permite la elevación de fotografías que justifiquen las entregas de los paquetes en el fichero diseñado para fotografiar los sellos de empresa, se ha detectado que algún mensajero, indebidamente y de forma desautorizada, ha incorporado al mismo la fotografía de algún Documento de Identidad, por lo que, en aras a prevenir cualquier acceso a imágenes no autorizadas, se ha suprimido el acceso a las carpetas indicadas de forma global y absoluta a cualquier usuario, tanto interno como externo.

CUARTO: Consecuencia de la identidad de los afectados y hechos la documentación incorporada al expediente E/00452/2018, fue acumulada al expediente de actuaciones previas E/00261/2018.

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 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."

III

El artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece:

"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".

Y el artículo 10 de la LOPD, relativo al deber de secreto señala 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";

"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".

IV

En el presente caso, el denunciante señala la existencia de una brecha de seguridad en la empresa denunciada dejando expuestos los datos personales de millones de personas al dejar sin seguridad los albaranes digitalizados de entrega de mensajería pudiendo acceder a los datos personales de sus destinatarios con tan solo cambiar el último número de la cifra que identificaba el albarán.

Hay que señalar que la propia empresa con anterioridad al escrito de denuncia informó el 20/12/2017 a la Agencia sobre los hechos denunciados y que estaban siendo investigados en el ámbito del expediente E/00261/2018. En el citado escrito se indicaba que había tenido constancia de la brecha de seguridad producida y que conocido el incidente de manera inmediata puso en marcha un protocolo de seguridad para restringir dicho acceso resolviendo el mismo; a continuación se ordenó una auditoria externa especializada en la detección de posibles ataques o vulnerabilidades del sitio web con el objeto de esclarecer los hechos y evitar incidentes similares y que se encontraban en un proceso de elaboración de un análisis forense para identificar la responsabilidad, medios y herramientas utilizadas en los accesos para ponerlo en conocimiento de las autoridades competentes, así como de la Agencia.

Posteriormente el 09/01/2018 ha informado de las medias adoptadas a fin de evitar que sucesos como el presente puedan volver a producirse y que se reproducen en el hecho tercero de la presente resolución y que acreditan la razonable diligencia mostrada por la entidad estableciendo protocolos más seguros.

Asimismo, se hace necesario poner de manifiesto la actuación poco ejemplarizante del denunciante, quien ha utilizado la información obtenida no únicamente con la finalidad de interponer la denuncia sino que, además, ha intentado conseguir un lucro con la misma al solicitar a la empresa una compensación económica.

En el caso examinado, no se ha constatado que la entidad denunciada haya incumplido la obligación de adoptar de manera efectiva las medidas dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros, por lo que no cabe entender infringido el artículo 9 de la LOPD citado, toda vez que actuó con razonable diligencia al informar de la brecha detectada y adoptar las medidas oportunas para impedir que se hicieran públicos los datos a través de la web, como ya se expone en párrafo anterior.

Procede tener en consideración la Sentencia de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional de fecha 25 de febrero de 2010 que, en relación con un caso similar al presente, señaló lo siguiente: *"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por el ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www..., descargándose una copia de la misma. Y tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.*

El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito del derecho administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1999, de 19 de diciembre (RTC 1991/246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de xxx".

No obstante, aunque en la citada Sentencia no se considera probada una vulneración del artículo 9 de la LOPD, sí se apreció una conducta infractora por parte del responsable del fichero, en concreto la vulneración del deber de guardar secreto, al considerar la tardanza de la entidad responsable en adoptar un comportamiento activo para impedir que se hicieran públicos en internet los datos personales comprometidos.

En el presente caso, en congruencia con la naturaleza atribuida a la figura del apercibimiento –alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella- cuyo objeto es la imposición de medidas correctoras, la Audiencia Nacional en numerosas sentencias concluye que cuando las medidas pertinentes ya hubieran sido adoptadas, lo procedente en Derecho será acordar el archivo de las actuaciones.

En este sentido, la sentencia de la A.N. de 29/11/2013 (Rec.455/2011), en su Fundamento de Derecho Sexto señala, a propósito de la naturaleza jurídica del apercibimiento regulado en el artículo 45.6 de la LOPD, que *"no constituye sanción"* y que se trata de *"medidas correctoras de cesación de la actividad constitutiva de la infracción"* que sustituyen a la sanción. La sentencia entiende que el artículo 45.6 de la

LOPD confiere a la AEPD una potestad diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

Por todo ello, en base a los principios de intervención mínima y proporcionalidad que informan la capacidad de actuación de esta Agencia y teniendo en cuenta que las medidas correctoras fueron ya adoptadas por iniciativa propia, en armonía con el pronunciamiento de la Audiencia Nacional recogido en la sentencia anterior deber acordarse el archivo de las actuaciones de investigación practicadas.

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a **GENERAL LOGISTICS SYSTEMS SPAIN SA** (antes Agencia Servicios Mensajería SA) y a ***B.B.B..***

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