Expediente Nº: E/04453/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad C.C.C. en virtud de denuncias presentadas por Don ***A.A.A.*** y por Doña ***B.B.B.***, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fechas 7 y 12 de julio de 2017 tienen entrada en esta Agencia denuncias presentadas por, respectivamente, Don ***A.A.A.*** y Doña ***B.B.B.*** (en lo sucesivo, los denunciantes), en la que manifiestan lo siguiente:

1. Uno de los denunciantes es madre de un alumno del centro denunciado y manifiesta que, con fechas 22 de febrero y 13 de marzo de 2017, recibió correos electrónicos de dicho centro en el que le comunicaban que con fecha 2 de febrero de 2017 se había producido una descarga ilícita de datos, que procedieron a investigar.

   En el correo del día 13 de marzo, la directora del centro manifestaba que "*la persona encargada del archivo informático y de la custodia de las bases de datos copiadas no se encontraba en el lugar de los hechos en el momento en que se produjo la descarga de los datos"*.

2. El otro denunciante es un profesor del centro que había prestado sus servicios hasta el día 6 de marzo de 2017, al cual le han sido imputados por el centro los hechos denunciados. Manifiesta que los datos descargados corresponden a un gran número de alumnos, en su gran mayoría menores de edad.

   Los hechos ocurridos el día 2 de febrero de 2017 se refieren a una brecha de seguridad en los equipos del centro. Una de las trabajadoras recibió una notificación del servidor avisando de un cambio de contraseña de acceso a la cuenta "***CUENTA.1", la cual aloja bases de datos de "Boletín Actividades C.C.C.", así como bases de datos de "Patronos C.C.C.", comprobando que dichas bases se habían exportado, es decir, que se había producido una salida no autorizada de información de nombres y correos electrónicos tanto de trabajadores como de patronos y familias del colegio.

   Tras comprobar que dicho cambio de contraseña no había sido autorizado, comienza una investigación de la que el centro deduce que el responsable es el denunciante.

3. La investigación se encarga a los servicios técnicos de la plataforma MAILCHIP, al proveedor de correo electrónico GOOGLE y a la plataforma externa T.A. OMICRON. Los hechos fueron denunciados ante la Policía.

4. Hasta ese momento, el Centro no contaba con ningún protocolo de Protección de Datos ni de uso de las herramientas informáticas, siendo reconocido por el propio centro este hecho, el cual hizo entrega con fecha 24 de marzo de 2017 de un protocolo, según figura en correos adjuntos a la denuncia como documentos 5 y 6, donde consta que dicho procedimiento se ha realizado a petición del Comité de Empresa.

5. Por otra parte, se denuncia la falta de formación de los empleados ni solicitud de suscripción de compromisos de confidencialidad por parte los mismos. Así mismo, denuncian falta de medidas de seguridad, en cuanto accesos, tiempo de bloqueo de ordenadores, etc.

Entre otra, anexan la siguiente documentación:

Copia de los correos electrónicos remitidos a los padres.
Copia de la Carta de despido del profesor del centro, donde se le imputan los hechos denunciados, tras las investigaciones realizadas por el centro.
Copia de la comunicación del delegado de administración con el envío a los trabajadores del Protocolo de Utilización de Herramientas Informáticas, confeccionado a raíz de los hechos.

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 (Informe E/04453/2017), teniendo conocimiento de los siguientes extremos:

Con fecha 21 de septiembre de 2017, se recibe escrito de C.C.C., en el que pone de manifiesto que:

a. Los ficheros descargados el 2 de febrero de 2017 fueron dos. Cada uno fue descargado dos veces. El primero, contenía nombres, apellidos y emails de padres y madres de alumnos y de empleados del centro. El segundo fichero contenía los nombres, apellidos y emails de los Patronos de la Fundación.

b. La descarga se produjo desde la cuenta que la C.C.C. mantiene en el servidor de correo electrónico “Mailchip”, para la confección y envío de su Boletín de Actividades (“newsletter”).

c. Con fecha 2 de febrero, la responsable de la “newsletter” recibió un correo automático de MAILCHIP, en el que le notificaba un cambio de contraseña no realizado por ella, seguido de otros correos que notificaban la descarga de los datos. Dicha responsable comunicó los hechos al responsable de seguridad, el cual impulsó una investigación de los hechos por parte del Departamento de Informática.

d. Las medidas de seguridad implantadas por C.C.C. con relación al acceso y tratamiento de los datos contenidos en sus ficheros son las siguientes:

i. Relación de prestadores de servicios con acceso remoto autorizado a los sistemas de información de la C.C.C., permitiendo la aplicación de las mismas medidas de seguridad, equivalentes a una conexión en área local (Anexo B del Documento de Seguridad adjunto).
ii. Con relación al régimen de trabajo fuera de los locales de la ubicación del fichero, según consta en el Anexo C del Documento de Seguridad, relativo a los portátiles autorizados a trabajar fuera de los locales, desde los que se debe reportar la siguiente información para poder acceder:
    Nombre de usuario con material asignado
    Apellido del usuario
    Línea asignada
    Modelo de terminal asignado
    Marca del portátil asignado
    Equipo validado por el Departamento IT
    Ubicación del usuario

e. Los usuarios son dados de alta únicamente por el responsable de seguridad o persona delegada y asociados a los diferentes perfiles, definidos por los niveles de acceso a las aplicaciones.

f. Será el Director de Administración quien tenga la última decisión sobre los derechos de acceso de los usuarios. Cada usuario deberá identificarse con usuario y contraseña tipo Gmail (Licencia Google Apps for Education). Cada usuario tiene atribuidos uno o más roles.

g. Para el primer acceso al sistema, el responsable de seguridad deberá comunicar de forma confidencial su identificador y su contraseña de acceso inicial, según las indicaciones en la norma sobre gestión de contraseñas.

h. C.C.C. mantendrá una relación actualizada de todos los usuarios con acceso autorizado al sistema informático, siendo responsabilidad del Departamento de Administración.

i. Según consta en el Anexo E, existen terceras empresas que acceden periódicamente a sus instalaciones, concretamente donde se encuentran ubicados los sistemas informáticos, en el caso de que se produjera un acceso de este tipo, el personal ha sido informado de su obligación de control y el responsable de tecnología se encargará de la autorización previa al acceso.

j. C.C.C. proporciona información a sus trabajadores, relativa a normas de utilización de los sistemas de información. Específicamente a través un comunicado interno y del correspondiente compromiso de confidencialidad.

k. El servidor “Mailchimp” tenía como única usuaria de la cuenta del centro a una responsable, no obstante el día que se produjo la descarga, ésta fue

realizada por una tercera persona que consiguió entrar en el correo de la responsable para activar el procedimiento de cambio de contraseña.

l. C.C.C. comunicó los hechos acaecidos a todos los miembros del Patronato a través de un correo electrónico informativo, cuya copia se adjunta como documento 5. Así mismo mandó una comunicación, que también se adjunta, como documento 6, a los padres, mediante la aplicación “Phidias”, a la que acceden mediante usuario y contraseña.

m. Con relación a las medidas correctoras para evitar los hechos ocurridos en el futuro, manifiestan que C.C.C. ha establecido un protocolo de utilización de herramientas informáticas específico. Así mismo, se han establecido controles de seguimiento informático con los datos de carácter personal que se almacenan en los equipos informáticos para la constatación de la correcta implantación de las medidas establecidas en el Reglamento 17/2007 de desarrollo de la Ley 15/1999 de Protección de Datos.

TERCERO: Consultada el 26 de enero de 2018 la aplicación de la AEPD que gestiona la consulta de antecedentes de sanciones y apercibimientos precedentes, a la entidad denunciada, C.C.C., no le constan registros previos.

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, 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 art. 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 aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

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.

Es necesario analizar las previsiones que el R. D. 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, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento 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*".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece que "*Todos los ficheros o tratamientos 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.

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 Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

Entre las medidas de seguridad de nivel básico, el Reglamento expone en su artículo 89.2, respecto de las funciones y obligaciones del personal, que: "*El*

responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento".

Así mismo, el artículo 91.3 del Reglamento, relativo al control de acceso, establece que: "*El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados*".

Por tanto, la no adopción de estas medidas de seguridad supone una infracción del citado artículo 9 de la LOPD.

La infracción se tipifica como grave en el artículo 44.3.h) de la LOPD como *"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*".

III

El artículo 45.6 de la LOPD establece:

"*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:

"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 IOS 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".*

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que la infracción de la LOPD de la que se responsabiliza a la entidad denunciada es "grave"; que la entidad denunciada no ha sido sancionada o apercibida por esta Agencia en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.4 de la LOPD: en concreto, la ausencia de beneficios obtenidos como consecuencia de la comisión de la infracción, la ausencia de intencionalidad y la inexistencia de perjuicios causados a las personas interesadas o a terceras personas. Así mismo, la entidad denunciada ha regularizado la situación irregular de forma diligente (45.5.b de la LOPD). Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.

IV

La Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección Primera, recurso 455/2011, de 29/11/2013, analiza el apercibimiento como un acto de naturaleza no sancionadora, como se deduce del fundamento de derecho

SEXTO:

"Debe reconocerse que esta Sala y Sección en alguna ocasión ha calificado el apercibimiento impuesto por la AEPD, en aplicación del artículo examinado, como sanción (SAN de 7 de junio de 2012, rec. 285/2010), y en otros casos ha desestimado recursos contencioso-administrativos interpuestos contra resoluciones análogas a la recurrida en este procedimiento, sin reparar en la naturaleza no sancionadora de la medida expresada (SSAN de 20 de enero de 2013, rec. 577/2011, y de 20 de marzo de 2013, rec. 421/2011). No obstante, los concretos términos en que se ha suscitado la controversia en el presente recurso contencioso-administrativo conducen a esta Sala a las conclusiones expuestas, corrigiendo así la doctrina que hasta ahora venía presidiendo la aplicación del artículo 45.6 de la LOPD."

Además, la sentencia interpreta o liga apercibimiento o apercibir con el requerimiento de una actuación para subsanar la infracción, y si no existe tal requerimiento, por haber cumplido las medidas esperadas relacionadas con la infracción, no sería apercibimiento, sino archivo, como se deduce del mencionado fundamento de derecho:

"Pues bien, en el caso que nos ocupa el supuesto concreto, de entre los expresados en el apartado quinto del artículo 45, acogido por la resolución administrativa recurrida para justificar la aplicación del artículo 45.6 de la LOPD es el primero, pues aprecia "una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

Por ello, concurriendo las circunstancias que permitían la aplicación del artículo 45.6 de la LOPD, procedía "apercibir" o requerir a la denunciada para que llevara a cabo las medidas correctoras que la Agencia Española de Protección de Datos considerase pertinentes, en sustitución de la sanción que de otro modo hubiera correspondido.

No obstante, dado que resultaba acreditado que la denunciada por iniciativa propia había adoptado ya una serie de medidas correctoras, que comunicó a la Agencia Española de Protección de Datos, y que esta había verificado que los datos del denunciante no eran ya localizables en la web del denunciado, la Agencia Española de Protección de Datos no consideró oportuno imponer a la denunciada la obligación de llevar a cabo otras medidas correctoras, por lo que no acordó requerimiento alguno en tal sentido a ésta.

Recuérdese que al tener conocimiento de la denuncia la entidad denunciada, procedió por iniciativa propia a dirigirse a Google para que se eliminara la URL donde se reproducían la Revista y el artículo, a solicitar a sus colaboradores que suprimieran cualquier nombre de sus artículos o cualquier otra información susceptible de parecer dato personal y que revisaran las citas del área privada de la web para borrar cualquier otro dato sensible, y, por último, a revisar la configuración de los accesos para que los buscadores no tuvieran acceso a las Revistas.

En consecuencia, si la Agencia Española de Protección de Datos estimaba adoptadas ya las medidas correctoras pertinentes en el caso, como ocurrió, tal y como expresa la resolución recurrida, la actuación administrativa procedente en Derecho era al archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, pues así se deduce de la correcta interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

Por el contrario, la resolución administrativa recurrida procedió a "apercibir" a la entidad PYB ENTERPRISES S.L., aunque sin imponerle la obligación de adoptar medida correctora alguna, lo que solo puede ser interpretado como la imposición de un "apercibimiento", entendido bien como amonestación, es decir, como sanción, o bien como un mero requerimiento sin objeto. En el primer caso nos hallaríamos ante la imposición de una sanción no prevista en la LOPD, con manifiesta infracción de los principios de legalidad y tipicidad en materia sancionadora, previstos en los artículos 127 y 129 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en el segundo supuesto ante un acto de contenido imposible, nulo de pleno derecho, de conformidad con lo previsto en el artículo 62.1.c) de la misma Ley."

La entidad denunciada ha adoptado medidas correctoras, como son el establecimiento de un protocolo de utilización de herramientas informáticas específico y de controles de seguimiento informático en relación con los datos de carácter personal que se almacenan en los equipos informáticos para la constatación de la correcta implantación de las medidas reglamentariamente exigidas. Por ello, resulta obligado, en atención a la citada sentencia de la Audiencia Nacional de 29/11/2013, interpretar, en congruencia con la naturaleza atribuida al apercibimiento, que siendo la finalidad del mismo la imposición de medidas correctoras, cuando éstas ya hubieran sido adoptadas, lo procedente en Derecho es acordar el archivo de las actuaciones. En el presente supuesto no cabe sino el archivo del procedimiento por haberse tomado medidas correctoras.

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 C.C.C., a Don ***A.A.A.*** y a Doña ***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