Procedimiento Nº AP/00042/2013

RESOLUCIÓN: R/00066/2014

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00042/2013**, instruido por la Agencia Española de Protección de Datos a la **CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX),** vista la denuncia presentada por Don ***A.A.A.***, y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 13 de noviembre de 2012, tuvo entrada en esta Agencia escrito de Don ***A.A.A.*** (en lo sucesivo el denunciante) en el que denuncia que el Instituto XXXXXXXXXX de Orihuela (Alicante) ha publicado en la dirección de su página web http://....., en abierto y a la vista de cualquiera los datos personales relativos a todos los profesores y alumnos del centro.

Adjunto a su denuncia aportó copia impresa de una muestra de los documentos que se publican en la citada página, en los que constan los datos de nombre y apellidos de profesores junto con sus horarios de clase y su cargo, así como el número de D.N.I. o N.I.E., los nombres y apellidos, fecha de nacimiento, nacionalidad, país de estudios previos y situación laboral de alumnos.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se realizaron las siguientes actuaciones:

1. Con fecha 7 de diciembre de 2012, se comprobó que los documentos objeto de la denuncia, se encontraban publicados en la página web http://..... de acceso público.

2. Con fecha 6 de febrero de 2013, el I.E.S. XXXXXXXXXX, perteneciente a la CONSELLERÍA D'EDUCACIO, CULTURA I SPORT de la Comunidad Valenciana, remitió, a requerimiento de esta Agencia, la siguiente información en relación con los hechos denunciados:

   - El Centro educativo tenía con anterioridad su página web ubicada en la dirección http://.....1. En la actualidad su página web se encuentra ubicada en la dirección http://..... El servidor se encontraba físicamente en el propio Centro, no obstante en el año 2011, cumpliendo las instrucciones de la Consellería de Educación se migró a los servidores Centrales de la citada Consellería.

   - El Centro, al igual que el resto de los que pertenecen a la mencionada Consellería, no dispone de servicios informáticos propios, por lo que ha

concertado dichos servicios con la empresa TECNAUSA el mantenimiento de una aplicación denominada SDGWEB, ubicada en la dirección http;///www.sgdweb.com/elpalmeral, en la que de forma personalizada con usuario y contraseña y previa autorización de los padres/madres/tutores de los alumnos éstos pueden acceder a toda la información relacionada con el ámbito educativo como exámenes, calificaciones, faltas de asistencia. Aportan copia impresa de la página web de acceso a la citada información.

- Además, al inicio del curso, en el sobre de matrícula se entrega una solicitud, en la que se pide autorización a los padres/madres/tutores de los alumnos para que en caso de que se realicen fotografías o grabaciones de sus hijos en las diversas actividades del centro, éstas puedan ser publicadas.

- En la ficha de matrícula donde se cumplimentan todos los datos personales, consta una leyenda informativa sobre el tratamiento de dichos datos y se informa sobre el ejercicio de los derechos ARCO, según lo dispuesto en la Ley Orgánica de Protección de Datos 15/1999.

- Asimismo, el Centro realiza todos los años la Prueba de Acceso a Ciclos, en cuya solicitud se autoriza el tratamiento informático de los datos que se facilitan, según consta en la leyenda incluida en el formulario de solicitud. Al tratarse de una prueba a nivel nacional, en la que el año pasado se matricularon más de 1000 alumnos provenientes de diferentes Comunidades Autónomas, se acordó publicar los resultados en la página web para evitar desplazamientos y gastos a todos ellos.

- Respecto a los diferentes formularios de recogida de datos utilizados en el Centro, aportan copia de los siguientes documentos:

  a. Solicitud de inscripción a pruebas de acceso a ciclos formativos, publicados en DOCV y del Impreso de ficha de matrícula. (en ambos consta una leyenda informativa en relación con lo establecido en el art. 5 de la LOPD.

  b. Impreso autorización envío datos vía web de alumnos y de envío de incidencias a través de SMS, en la que el representante legal del alumno autoriza al Centro para que la información de los datos académicos del alumnos se remita a la plataforma web accesible a través de internet, para ser consultada por las personas autorizadas, previa solicitud de contraseña.

  c. Impreso autorización de publicación de fotografías y vídeos de alumnos que correspondan a actividades organizadas por el Centro.

- La Programación General Anual (P.G.A.) es el documento resumen de todos los aspectos que regirán el curso: horario del profesorado, grupos, alumnos,

estadísticas sobre resultadas académicos de cursos anteriores etc…

- De acuerdo con las instrucciones de inicio de curso de la Consellería d'Educación de fecha 17/08/2012 (de obligado cumplimiento), cuya copia adjuntan, la P.G.A. se tiene que poner en conocimiento de los diferentes miembros de la comunidad educativa.

- La inclusión de la P.G.A. en la página web del Centro se informó previamente tanto en el Claustro de Profesores como en el Consejo Escolar, donde están representados los alumnos, padres/madres, personal no docente, ayuntamiento y profesores, sin ningún tipo de oposición ni voto particular al respecto. A este respecto han aportado la siguiente documentación:

  d. Certificado del Secretario del Centro, sobre el contenido del Acta aprobada del Claustro Extraordinario de 16 de diciembre de 2012, en la que consta "Se ha subido la PGA a la web del Centro tal y como se informó previamente en el tablón de la Sala de Profesores".

  e. Nota informativa del Director del Centro (no consta la fecha), en la que informa que quedan desconvocadas las sesiones de Claustro y Consejo de los días 9 y 13 para cumplir con los plazos establecidos respecto al tiempo de exposición del documento PGA, que no ha podido ser puesto a disposición de la comunidad educativa hasta el día 7 y que se encuentra publicado tanto en la Sala de profesores como en la página web del centro.

- El contenido del documento PGA está definido por el programa informático de la Consellería d'Educació sin que se pueda modificar por parte de los Centros, debiendo estos, remitir una versión digital a la Dirección Educación de Alicante y conservar una versión en papel en la Secretaría del Centro, la cual está a disposición de quien lo solicite, dado que se trata de un documento público.

- Hasta la fecha no han recibido ninguna solicitud de acceso, rectificación, cancelación u oposición, según lo dispuesto en la Ley Orgánica 15/1999, en relación con la publicación de dichos datos.

- Con respecto al órgano responsable de la publicación de documentos oficiales en la web, es el propio Centro, a través de la Secretaría, que es quien gestiona toda la documentación, de acuerdo con las competencias de la ley.

- Actualmente se encuentran en proceso de adecuación de la página web de forma que se asegure el acceso a la información a través de la correspondiente identificación de usuario y contraseña y en la sección de

secretaría se está procediendo a realizar los cambios que aseguren el acceso personalizado.

- Por último manifiestan que desde el propio Centro y de acuerdo con las instrucciones que reciben desde la Consellería d'Educació, se trata de cumplir con las normas de protección de datos y del derecho a la propia imagen, y que al tener conocimiento de las presentes actuaciones han deshabilitado el acceso a través de la web a los documentos que todavía eran accesibles.

TERCERO: Con fecha 30 de septiembre de 2013**,** el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a la CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX) por la presunta infracción de los artículos 9.1 y 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en los artículos 44.3.h) y 44.3.d), respectivamente, de dicha norma.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, en fecha 24 de octubre de 2012, la Consellería de Educación presentó escrito de alegaciones adjuntando informe jurídico realizado por la Abogacía General de la Generalitat Valenciana en el que, en síntesis, manifestaba lo siguiente:

- Entre la AEPD y la Administración del Consell no existe una relación de potestad; por ello la AEPD no puede ejercitar la potestad sancionadora sobre las administraciones públicas sino que, según dispone el art 46 de la LOPD, únicamente puede dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción.
- Por lo tanto, la utilización del Real Decreto 1398/1993, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la Potestad sancionadora e este caso es totalmente improcedente ya que no se está ejercitando potestad sancionadora como expresa la Ley 30/92, respecto a la garantía del procedimiento en su artículo 134: "*1. El ejercicio de la potestad sancionadora requerirá procedimiento legal o reglamentariamente establecido".*
  En este caso al utilizar un procedimiento sancionador totalmente inadecuado la AEPD incurre en un vicio de nulidad absoluta.
- Falta de concreción de hechos e imposibilidad de alegaciones.
- Que del acuerdo de inicio no se desprende qué medidas de seguridad ha incumplido la Consejería mediante la publicación en la página web.
- Que el deber de secreto se debe atribuir a una persona concreta respecto a de una información determinada que sea secreta y que el IES XXXXXXXXXX no es un sujeto apto para infringir el deber de secreto.

Con fecha 25 de octubre la Consellería de Educación presentó un nuevo escrito de alegaciones en el que, básicamente, manifestaba lo siguiente:

- Que la PGA es un documento recogido en la Ley Orgánica de Educación

(LOE) que en su artículo 125 establece que los centros educativos elaborarán a principio de cada curso una PGA que recoja todos los aspectos relativos a la organización y funcionamiento del centro incluidos proyectos, currículos, normas y planes de actuación acordados y aprobados.

- El artículo 127.b) de la LOE establece la competencia para aprobar y evaluar el PGA al Consejo escolar del centro…
- Que en las instrucciones de inicio del curso 2012-2013, el D. G. de Innovación y Ordenación estableció el traslado de la propuesta de PGA por vía electrónica o telemática.
- Que tanto la LOE como la Consellería de Educación manifiestan la necesidad de publicitar y recabar propuestas de todos los sectores.
- El contenido de la PGA puesto a disposición es íntegramente el que tenía que ser elaborado, debatido y aprobado.
- El profesor denunciante en los cursos previos en que ha estado en este centro no manifestó oposición alguna al procedimiento, curiosamente la fecha en que se produce la denuncia coincide con la existencia de una problemática laboral-disciplinaria que afectaba a dicho profesor.
- Por todo lo anterior, quiere dejar constancia de que se ha actuado con el convencimiento de la corrección en todo el proceso y que, en cuanto se tuvo conocimiento de la posibilidad de incorrección no deseada, ésta fue eliminada.

QUINTO: Con fecha 28 de octubre de 2013, se acordó por la Instructora del procedimiento la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, E/07984/2012, así como la documental aportada por la CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX).

Asimismo, se dio por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio AP/00042/2013 presentadas por la CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX), y la documentación que a ellas acompaña.

También se incorporó al procedimiento Informe de situación de inscripción en el Registro General de Protección de Datos referidos a los ficheros de Alumnos y Personal docente, pertenecientes a la Consejería de Educación de la Generalitat Valenciana que constan con Medidas de Seguridad Nivel Básico.

SEXTO: Con fecha 2 de diciembre de 2013, la Instructora del procedimiento emitió Propuesta de Resolución, en el sentido de que por el Director de la Agencia Española de Protección de Datos se declare que la CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX) ha infringido lo dispuesto en los artículos 9.1 y 10 de la LOPD, lo que supone una infracción tipificada como grave en los artículos 44.3.h y 44.3.d), respectivamente, de la citada norma, así como que se requiera la adopción de las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de los artículos 9.1 y 10 de la mencionada Ley.

SÉPTIMO: Con fecha de entrada en la Agencia el 8 de enero de 2014, la Consellería de Educación realizó alegaciones frente a la citada propuesta de resolución en las que

manifiesta que no se formulan otras distintas a las ya remitidas por el IES XXXXXXXXXX y comunica que se han adoptado las siguientes medidas:

- *"En cuanto se tuvo conocimiento de la posibilidad de que en la información ubicada en la web del centro pudiera contener elementos no suficientemente protegidos, se procedió inmediatamente a su retirada tal y como se indicó en el pliego de alegaciones formuladas por el Director del IES XXXXXXXXXX.*
- *Desde esa fecha no figura en la citada web, información alguna susceptible de no cumplir los requeridos por la Ley de Protección de Datos"*

HECHOS PROBADOS

PRIMERO: Don ***A.A.A.*** denunció ante la Agencia que el Instituto XXXXXXXXXX de Orihuela (Alicante) publicó en la dirección de su página web http://....., en abierto y a la vista de cualquiera los datos personales relativos a todos los profesores y alumnos del centro relativos al PGA 2012-2013 (folios 1-17).

SEGUNDO: Con fechas 7 de diciembre de 2012 y 9 de enero de 2013, la Inspección de Datos verificó que los documentos objeto de la denuncia, se encontraban publicados en la página web http://..... de acceso público (folios 81-85)

TERCERO: Los datos personales publicados son los siguientes: nombre y apellidos de profesores junto con sus horarios de clase y su cargo, así como el número de D.N.I. o N.I.E., los nombres y apellidos, fecha de nacimiento, nacionalidad, país de estudios previos y situación laboral de alumnos – la mayoría de ellos menores - (folios 9-17 y 82, entre otros).

CUARTO: Los ficheros de Alumnos y Personal docente publicados, constan inscritos en el Registro General de Protección de Datos con Medidas de Seguridad Nivel Básico (folios 119-121).

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

Procede en primer lugar analizar las alegaciones de la Consellería de Educación según las cuales la AEPD incurre en vicio de nulidad ya que no puede ejercitar la potestad sancionadora sobre las administraciones públicas sino que únicamente puede dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Y que, por lo tanto, la utilización del Real Decreto 1398/1993, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la Potestad sancionadora en este caso es totalmente improcedente ya que no se está

ejercitando potestad sancionadora como expresa la Ley 30/92, respecto a la garantía del procedimiento en su artículo 134: "*1. El ejercicio de la potestad sancionadora requerirá procedimiento legal o reglamentariamente establecido".*

A este respecto hay que significar que el artículo 46 de la LOPD indica:

"*1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera…*".

Por su parte, en el Título IX, Capítulo III, Sección 3ª del 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, se establece el Procedimiento Sancionador, en sus artículos 127 y 128. Y en su Sección 4ª, del mismo Capítulo (Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las Administraciones públicas), recoge en su artículo 129 lo siguiente:

"*Disposición general.-El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo".*

El presente procedimiento se ha tramitado y, así se informó en el Acuerdo de Inicio, con arreglo a lo dispuesto en el artículo 46 de LOPD, por la presunta infracción de los artículos 9.1 y 10 de dicha norma, tipificadas como graves en el artículo 44.3.h) y 44.3.d), respectivamente, de la citada Ley Orgánica.

Por lo tanto, dichas alegaciones deben ser desestimadas.

III

Por lo que respecta a las alegaciones al acuerdo de inicio, según las cuales la Consellería ha manifestado que ha actuado con el convencimiento de la corrección en todo el proceso, procede señalar lo siguiente:

El principio de culpabilidad es exigido en el procedimiento sancionador y así la STC 246/1991 considera inadmisible en el ámbito del Derecho administrativo sancionador una responsabilidad sin culpa. Pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada y a este respecto el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dispone *"sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable*." El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento*

típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia." (STS 23 de enero de 1998).

A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que *"basta la simple negligencia o incumplimiento de los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia..."*(SAN 29de junio de 2001).

IV

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."

V

Se imputa a la CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX), responsable de los ficheros de profesores y alumnos, 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.

Y 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 la Consellería de Educación de los usuarios que acceden a los ficheros de Profesores y Alumnos, correspondiendo adoptar las calificadas de nivel bajo, en atención al tipo de información básica 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.

Por otra parte, el artículo 90 del mismo reglamento, aplicable igualmente a los ficheros de nivel básico de seguridad, se refiere al registro de incidencias señalando lo siguiente:

"Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas".

En definitiva, la Consellería de Educación, responsable de los ficheros Profesores y Alumnos, 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, sin embargo, ha quedado acreditado que la citada entidad incumplió esta obligación, por cuanto el Instituto XXXXXXXXXX colgó en su página web, en abierto y a la vista de cualquiera, los datos personales relativos a los ficheros de Profesores y Alumnos y no impidió de manera

fidedigna que el denunciante pudiera acceder a datos personales de otros ciudadanos que se hubiesen registrado a través de dicho canal.

En concreto, consta que en el mes de noviembre de 2012, el denunciante accedió a la página web http://....., comprobando que se mostraban datos personales, laborales y académicos de terceros, relativos al Curso escolar 2012-2013. Además, con fechas 7 de diciembre de 2012 y 9 de enero de 2013, la Inspección de datos verificó que los documentos objeto de la denuncia, continuaban publicados en la página web http://..... de acceso público (folios 81-85). Los datos personales publicados son los siguientes: nombre y apellidos de profesores junto con sus horarios de clase y su cargo, así como el número de D.N.I. o N.I.E., los nombres y apellidos, fecha de nacimiento, nacionalidad, país de estudios previos y situación laboral de alumnos – la mayoría de ellos menores - (folios 9-17 y 82, entre otros).

Por tanto, el mecanismo de acceso a la información contenida en el sistema no cumplió las exigencias contenidas en los artículos antes reseñados, sobre control de accesos, identificación y autenticación de usuarios, por cuanto mostró datos personales que no pertenecían a un usuario identificado.

Así, los datos personales de los comprobando que, asociados a su perfil, se mostraban datos personales, laborales y académicos de terceros eran accesibles desde la zona habilitada para los mismos, 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"*.

En consecuencia, se considera que la Consellería de Educación (IES XXXXXXXXXX) ha incurrido en la infracción grave descrita.

Tales hechos quedaron acreditados por la documentación aportada por el denunciante, que incluía el detalle de la información accedida a través de la página web del Instituto.

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".*

VI

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 la Consellería de Educación ha incurrido en la infracción grave descrita.

VII

En segundo lugar, se imputa a la Consellería de Educación la infracción del artículo 10 de la LOPD que dispone lo siguiente: "*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 tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así, el Tribunal Superior de Justicia de Madrid declaró en su sentencia de 19 de julio de 2001: "*El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".*

En este sentido, la Audiencia Nacional también ha señalado, entre otras, en sentencias de fechas 14 de septiembre de 2001 y 29 de septiembre de 2004 lo siguiente: *"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 CE.*

En efecto, este precepto contiene un <<instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute 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>> (*STC 292/2000). Derecho fundamental a la protección de los datos que <<persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino>> (STC 292/2000) 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>>.*

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible.

El Tribunal Superior de Justicia de Madrid, en su sentencia de 16 de octubre de 2001, reitera que "*el TC en su Sentencia 76/1990, de 26 de abril, nos recuerda que, aún sin reconocimiento explícito en la Constitución, el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (art. 25.1 CE) o de las exigencias inherentes al Estado de Derecho; manifestando la STC 246/1991, de 19 de diciembre, que es inadmisible en el ámbito del derecho administrativo sancionador una*

responsabilidad sin culpa. La Ley 30/92 ha pretendido regular la cuestión en su artículo 130.1 al consagrar el principio de responsabilidad como uno de los informadores del ejercicio de la potestad sancionadora, estableciendo que "sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia"; el último inciso "aún a título de simple inobservancia" no es muy preciso puesto que pudiera pensarse que consagra una responsabilidad objetiva sin dolo o culpa del sujeto, por lo que deberá interpretarse conforme a la doctrina aludida, así como señala la más reciente jurisprudencia del Tribunal Supremo (SS 16 y 22 de abril de 1991 y 5 de febrero de 1992) uno de los principales componentes de la infracción administrativa es el elemento culpabilista, del que se desprende que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable.- Probablemente, el legislador de la Ley 30/92 haya pretendido aludir a que serán sancionables las infracciones meramente formales, aunque no produzcan un resultado dañosos al interés público e, igualmente, que será incriminable la culpa inconsciente o sin representación, atendiendo al aspecto normativo de la culpabilidad según el cual puede reprocharse no haber previsto lo que se podía y debía prever." Consiguientemente, aún en el supuesto en que se hubiera padecido algún tipo de error, el mismo constituiría una falta de diligencia plenamente imputable a la entidad sancionada, con claro incumplimiento del artículo 10 (...) tipificado correctamente y sancionado como falta grave (...)."

En el presente caso consta acreditado que, al menos entre el mes de octubre de 2012 y el 9 de enero de 2013, la Consellería de Educación (IES XXXXXXXXXX) publicó en su página web http://....., los datos personales, laborales y académicos de los ficheros Profesores y Alumnos, relativos al Curso escolar 2012-2013. Los datos personales publicados son los siguientes: nombre y apellidos de profesores junto con sus horarios de clase y su cargo, así como el número de D.N.I. o N.I.E., los nombres y apellidos, fecha de nacimiento, nacionalidad, país de estudios previos y situación laboral de alumnos – la mayoría de ellos menores - (folios 9-17 y 82, entre otros).

Por otra parte, la Consellería no ha acreditado ante esta Agencia que contara con el consentimiento de los titulares de los datos para la publicación en la página web que se detalla más arriba.

Por tanto, se incumplió el deber de secreto con la revelación de datos personales a terceros con motivo de la publicación en cuestión, que puede calificarse como un incumplimiento de lo dispuesto en la normativa de protección de datos; quedando acreditado en el expediente que los datos personales los ficheros Profesores y Alumnos en poder de la Consellería de Educación fueron difundidos sin su consentimiento ni habilitación legal para ello, por lo que ha de entenderse vulnerado el deber de secreto que impone el artículo 10 de la LOPD.

VIII

El artículo 44.3.d) de la LOPD, califica como infracción grave:

"La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley".

De acuerdo con los fundamentos anteriores, hay que entender que por parte de la Consellería de Educación se ha producido una vulneración del deber de secreto, dado que la información difundida contiene datos de carácter personal concerniente a

terceros, y que procede calificar la infracción como infracción grave.

En este procedimiento se ha acreditado que la entidad imputada ha divulgado los datos personales contenidos en la relación cuestionada en este procedimiento al permitir el acceso sin limitación alguna a los mismos.

Dado que ha existido una vulneración en el deber de secreto por parte del denunciado en relación a datos personales, se considera que ha incurrido en la infracción descrita.

El hecho constatado de la difusión de los datos personales ya citados fuera del ámbito del imputado, establece la base de facto para fundamentar la imputación de las infracciones de los artículos 9 y 10 de la LOPD.

No obstante, nos encontramos ante un supuesto en el que un mismo hecho deriva en dos infracciones, dándose la circunstancia de que la comisión de una implica necesariamente la comisión de la otra. Esto es, con la difusión en internet de los datos personales citados en abierto sin limitación de los accesos y sin el consentimiento de los afectados, se está produciendo un incumplimiento de las medidas de seguridad exigidas a dicho responsable que, a su vez, deriva en una vulneración del deber de secreto.

Por lo tanto, aplicando el artículo 4.4 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora que señala que "*en defecto de regulación específica establecida en la norma correspondiente, cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*", procede subsumir ambas infracciones en una. Dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.d) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD por considerar que resulta la infracción originaria.

El concurso de infracciones en los procedimientos de infracción de las Administraciones Públicas ha sido puesto de relieve por la Audiencia Nacional en su Sentencia de 23/11/2012 (recurso 346/2011), en el Fundamento Jurídico sexto: "*Considera el Abogado del Estado en representación de la Agencia Española de Protección de Datos, que resulta inaplicable el artículo 4.4 del Reglamento de procedimiento sancionador, porque no hay dos sanciones al tratarse de una Administración pública, y se sustituye la imposición de sanción en virtud del artículo 46.1 de la Ley.*

En el presente caso efectivamente consta que los datos estaban disponibles en un documento de otra página web de un estudio de arquitectos, por lo que se produce el supuesto de revelación.

En segundo lugar, respecto al sujeto responsable de la infracción, en otras sentencias anteriores de esta Sala, así en la Sentencia de 19 de octubre de 2010 (rec. 391/2009), se imputa la infracción al responsable del fichero, aún por la intervención de tercero a quien contrató:

"En el supuesto que nos ocupa es un hecho constatado que los ficheros de los clientes de la empresa se encontraban en la vía pública esparcidos por la calle, incumpliéndose la obligación que tenía el responsable del fichero de adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad del dato, lo que determinó que los datos personales de sus clientes pudieran ser vistos por cualquier persona que transitase por la vía pública. No se ha podido constatar si el abandono de esta documentación se produjo por empleados de la propia empresa, por el nuevo ocupante del local al realizar las obras de acondicionamiento o, tal y como afirma la parte recurrente, por los responsables de la empresa contratada para la destrucción de la documentación, pero lo cierto es que la empresa responsable del fichero incumplió el deber de secreto y de custodia de tales datos aun cuando fuera por la intervención de tercero al que contrató para la prestación de un servicio de destrucción de la documentación".

Por tanto, también el responsable del fichero puede ser sujeto de la infracción por la revelación de datos por el encargado, pero, efectivamente, en otras ocasiones esta Sala ha conocido de recursos en los que se ha apreciado la existencia de concurso medial entre las infracciones de los arts. 44.3, apartados d) y h), LOPD, así en la Sentencias de esta Sala de 19 de octubre de 2010 (rec. 471/2009), de 3 de febrero de 2011 (rec. 45/2010), de 23 de junio de 2011 (rec. 367/2010), y en la Sentencia de 8 de abril de 2010 (rec. 760/2009), cuyo fundamento de Derecho 2.º, resuelve:

"La AEIT ha vulnerado el artículo 9 de la LOPD pues tenía que haber adoptado las medidas efectivas para impedir el acceso a los datos contenidos en los ficheros por parte de terceros y se constató una falta de medidas de seguridad en los ficheros que permitían visualizar las claves del administrador del sistema, posibilitando a través de la herramienta de gestión de bases de datos phpMyAdmin el acceso de terceros al sistema informático de gestión de los ficheros de la AEIT como administrador del sistema. La AEIT también vulneró el deber de secreto garantizado en el artículo 10 de la LOPD. No obstante, al estar ante un supuesto en el que existe un concurso medial de infracciones, dándose la circunstancia de que la comisión de una implica la comisión de la otra, aplicando el artículo 4.4 del Real Decreto 1398/93, procede subsumir ambas infracciones en una, procediendo imputar únicamente la infracción grave del artículo 9 de la LOPD ."

En este caso la revelación de datos por el encargado del fichero se está imputando al responsable del fichero, y ello precisamente por haber vulnerado éste las medidas de seguridad, por lo que, sin duda, en lo que se refiere a la responsable del fichero, procede apreciar que la comisión de una infracción (incumplimiento del deber de secreto) se ha derivado necesariamente de la otra (incumplimiento de medidas de seguridad), y, en consecuencia, aquélla se deberá subsumir en la infracción más grave, conforme al art. 4.4 del Real Decreto 1398/1993 por el que se aprueba el Reglamento de Procedimiento sancionador".

Por tanto, dado que, en este caso, se ha producido una vulneración de las medidas de seguridad, calificada como grave por el artículo 44.3.h) de la LOPD y también un incumplimiento del deber de guardar secreto, calificado como grave en el artículo 44.3.d) de la misma norma, procede imputar únicamente la infracción del artículo 9 de la LOPD por considerar que resulta la infracción originaria.

IX

Por último, el artículo 46 de la LOPD, *"Infracciones de las Administraciones Públicas"*, dispone que:

«1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.»

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

En el presente supuesto no se insta la adopción de medidas correctoras puesto que la Consellería de Educación ha subsanado la situación irregular y los efectos de la infracción cometida, ya que se procedió a la retirada de la página web de los datos personales publicados.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **DECLARAR** que la **CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX),** ha infringido lo dispuesto en el artículo 9.1 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

SEGUNDO: Debido a la naturaleza de la infracción no se insta por parte de la Agencia la adopción de una concreta medida correctora. No obstante se solicita se comuniquen las que de forma autónoma decida adoptar.

TERCERO: **NOTIFICAR** la presente resolución a la **CONSELLERÍA D´EDUCACIÓ, CULTURA I ESPORT DE LA GENERALITAT VALENCIANA (I.E.S. XXXXXXXXXX),** y a Don ***A.A.A..***

CUARTO: **COMUNICAR** la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

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, se podrá 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 lo sucesivo LJCA), 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la LJCA, sólo podrá interponer 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 LJCA, 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.

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