Compendio LOPD para Centros Educativos

Gesdatos Software, S.L
02/11/2011

Informes Jurídicos, Tutelas de Derechos y Preguntas más Frecuentes.

Índice.

INTRODUCCIÓN

El derecho fundamental a la protección de datos de carácter personal ha estado regulado, por primera vez nuestro ordenamiento jurídico, a través de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

Esta norma vigente hasta el 14 de enero de 2000, previó la creación de la Agencia Española de Protección de Datos (en adelante, AEPD), quedando conformada mediante el Real Decreto 428/1993, de 26 de marzo.

De este modo, la AEPD se ha constituido como un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, relacionándose con el Gobierno a través del Ministerio de Justicia.

Una de sus principales funciones, con carácter general, es velar por el cumplimiento de la legislación sobre protección de datos, esto es, las vigente Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante, LOPD) y sus normas de desarrollo y controlar su aplicación a fin de garantizar el derecho fundamental a la protección de datos personales.

Entre otras labores, se encuentra la elaboración de informes jurídicos respecto a las consultas planteadas por los responsables de ficheros (entidades públicas y privadas) en cuanto a la interpretación y aplicación de la LOPD, sus normas de desarrollo, así como otras normas que se interrelacionaran con la materia de protección de datos de carácter personal.

No obstante, debe significarse que dichos informes no tienen carácter vinculante y no prejuzgan el criterio del Director de la Agencia en el ejercicio de sus funciones, entre las que la Ley no prevé la evacuación de consultas vinculantes.

Además de la AEPD, se han creado autoridades de control autonómicas, en este caso, sólo las Agencias de Protección de Datos de la Comunidad de Madrid, Cataluña y País Vasco. Éstas únicamente tienen competencia respecto a los ficheros o tratamientos de datos personales de las entidades públicas de su circunscripción geográfica. Aunque con menor profusión, estos organismos autonómicos también emiten informes jurídicos. Más cabe decir, que en los informes jurídicos de las agencias autonómicas se interpreta y aplica la normativa de protección de datos, en consonancia con legislación autonómica, que no resulta de aplicación.

Sin embargo, todos estos informes han permitido arrojar luz a cuestiones complejas en el ámbito del sector educativo, en cuanto a la interpretación y aplicación de esta normativa. Bien de oficio o en contestación a consultas formuladas por los propios centros educativos (públicos, privados o concertados) la AEPD y las autoridades de control autonómicas han trazado la interpretación y aplicación de la LOPD, sobre todo, en conjugación con las diversas leyes en materia de educación.

GESDATOS en el estudio y análisis periódico de la legislación, presta máxima atención a los dictámenes emitidos por la autoridad de control estatal y las autonómicas.

Conocedores de los pronunciamientos de la AEPD y agencias autonómicas, GESDATOS ha realizado una labor de selección, de aquellos que pueden resultar de interés para el personal, tanto administrativo como educativo de los Centros).

A estos efectos, GESDATOS ha elaborado el presente compendio de informes jurídicos de la AEPD y las citadas autoridades de control autonómicas, el cual obedece a un criterio de ordenación y estructura por materias o áreas de un centro educativo. No habiendo informes relativos a todos los aspectos de un Centro Educativo, independientemente del nivel, se ha tratado de agrupar los más significativos por razón de la materia que versan y/o corresponden a una unidad o área concreta.

Este compendio se completa con resoluciones dictadas por la AEPD en relación a procedimientos sancionadores abiertos a Centros Educativos, ante un incumplimiento o supuesto incumplimiento de la normativa.

Y, asimismo, recoge una relación de pronunciamientos de nuestros tribunales (Audiencia Nacional, Tribunal Supremo y Tribunal Constitucional) en interpretación o aplicación de la legislación vigente en protección de datos.

El compendio no recoge todos los informes jurídicos y procedimientos sancionadores de la AEPD y agencias autonómicas de protección de datos, sólo aquéllos que a criterio de GESDATOS resultan de interés o relevancia para la administración pública local.

La AEPD y las agencias autonómicas publican informes jurídicos con cierta periodicidad. Es por esto que, a la entrega o puesta a disposición del compendio, se incluirán los últimos informes y procedimientos sancionadores de la AEPD, así como pronunciamientos de los tribunales, que se hubieren publicado o emitido hasta la fecha. GESDATOS realiza una labor de actualización, conforme a las emisiones o publicaciones de los citados organismos, de manera que puede haber varias ediciones o versiones del compendio.

En definitiva, el único propósito de GESDATOS es aportar, de este modo, un instrumento de ayuda y apoyo en nuestra labor de consultoría, para esclarecer cuestiones emergentes entorno a la aplicación de la normativa de protección de datos en el ámbito de una entidad local.

GESDATOS.

INFORMES JURÍDICOS.

Informe 143/2004 sobre: Responsable del fichero en la enseñanza pública.

La consulta plantea si el Centro consultante debe proceder a la notificación de sus ficheros a fin de lograr su inscripción en el Registro General de Protección de Datos o si tal obligación corresponde a la Consejería de la cual depende.
Como punto de partida, el artículo 5 del Real Decreto 1332/1994, de 20 de junio, declarado vigente por la Disposición transitoria tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, establece que "Todo fichero de datos de carácter personal, de titularidad pública, será notificado a la Agencia de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia, de una copia de la disposición de creación del fichero".
En consecuencia, la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".
Para determinar a quién corresponde la obligación de proceder a la adopción de la correspondiente disposición de carácter general y la consiguiente notificación del tratamiento al Registro General del Protección de Datos resulta imprescindible delimitar si el consultante es un órgano incardinado en la Administración Autonómica o si el mismo posee personalidad jurídica independiente de la misma.
En el primer supuesto, el Centro no sería sino un mero usuario del fichero, cuyo responsable sería la Administración educativa autonómica, de forma que la obligación de notificación correspondería a la Consejería de Educación, debiendo hacerse referencia al Centro educativo únicamente como lugar de ubicación del fichero. En caso contrario, el responsable del fichero sería el propio Centro, correspondiendo al mismo la notificación del tratamiento al Registro de esta Agencia.
Según dispone el artículo 64 de la Ley Orgánica 10/2002, de Calidad de la Educación "Los centros docentes se clasifican en públicos y privados", añadiendo que "Son centros públicos aquellos cuyo titular sea un poder público".
En consecuencia, la Ley Orgánica vincula el carácter público de los Centros con la titularidad de los mismos. Al propio tiempo, la misma no establece en ningún lugar si los centros tendrán o no personalidad jurídica dependiente de la correspondiente Administración Educativa, si bien especifican expresamente los ámbitos en que los mismos gozarán de autonomía pedagógica, organizativa y de gestión económica (artículos 67 a 70 de la Ley Orgánica).
En el ámbito de la Comunidad Autónoma, la normativa aplicable señala que los institutos de educación secundaria, dependientes de la Consejería de Educación y Ordenación Universitaria, son centros docentes públicos que podrán impartir una o varias etapas de las enseñanzas de educación secundaria, añadiendo que la creación y supresión de los institutos a los que se refieren los apartados anteriores corresponde al Gobierno mediante Decreto, a propuesta del consejero de Educación y Ordenación Universitaria".
De lo dispuesto en la legislación básica estatal y en la autonómica a la que acaba de hacerse referencia se desprende que los Centros Públicos de Enseñanza Secundaria no son sino órganos directamente dependientes de la Consejería autonómica y carentes de personalidad propia y diferenciada de la misma, sin prejuicio de las peculiaridades que les son propias en lo referente al respeto de los principios de autonomía pedagógica, organizativa y de gestión económica que la Ley establece.
Por ello, ha de concluirse que, integrados orgánicamente en la Administración autonómica, será ésta la obligada al cumplimiento delas obligaciones que respecto de los ficheros de titularidad pública impone la Ley Orgánica 15/1999, debiendo la misma

adoptar la correspondiente disposición de carácter general y proceder a la notificación de los tratamientos al Registro General de Protección de Datos, en la que se hará constar que el Centro es el lugar de ubicación del fichero.

Informe 466/2004 sobre: La comunicación a los padres de las calificaciones de sus hijos menores de edad.

La consulta plantea diferentes cuestiones relativas a la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, a los menores de edad.

I

En primer lugar, se plantea a qué edad pueden recabarse directamente de un menor sus datos personales, sin contar con la autorización de sus padres o tutores legales. En este sentido, la consultante solicita información sobre si la solución a dicha cuestión depende del tipo de dato personal de que se trate y, en consecuencia, del diferente nivel de protección que la Ley confiere al dato personal en atención a la naturaleza de la información tratada.

Planteado así el problema, deben analizarse las especialidades derivadas del hecho de que los datos personales sean recabados de personas menores de edad. En este sentido, debe señalarse como regla general que las disposiciones de la Ley Orgánica de Protección de Datos serán aplicables por igual, con independencia de la mayoría o minoría de edad de los afectados.

Ello no obstante, deberá analizarse en especial la prestación del consentimiento, exigido por la Ley para que el tratamiento de los datos sea conforme a Derecho, tal y como dispone el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Este consentimiento habrá de ser, tal y como exige el artículo 3 i) de la propia Ley, libre, específico, inequívoco e informado, siendo necesario el cumplimiento de lo preceptuado por el artículo 5.1, a cuyo tenor

"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

Lo que se ha venido indicando hasta ahora es predicable de cualquier tratamiento consistente en la recogida de datos de carácter personal de cualesquiera personas. Sin embargo, en el supuesto de que las personas de las que se obtienen los datos sean menores de edad, será necesario analizar en qué supuestos se considerará que los mismos ostentan pleno discernimiento para prestar ese consentimiento y en cuáles aquél habrá de completarse con el de su representante legal.

A nuestro juicio, deben diferenciarse dos supuestos básicos, el primero referido a los mayores de 14 años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el segundo, al consentimiento que pudieran prestar los menores de dicha edad.

Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".

Se plantea entonces si, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su

consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 para los mayores de catorce años.

Por otra parte, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en Resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.

En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal.

Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez.

De acuerdo con lo anterior, la solución al supuesto planteado por la consultante, esto es, la posibilidad de recabar directamente de un menor sus datos personales, sin contar con la autorización de sus padres o tutores legales, no depende del tipo de dato personal de que se trate, ni debe vincularse al diferente nivel de protección que la Ley confiere al dato personal en atención a la naturaleza de la información tratada y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. Por el contrario, la solución a cada caso concreto se extraerá de lo expuesto anteriormente en relación con los mayores de catorce años, y de las condiciones de madurez del menor de dicha edad, de acuerdo con lo establecido en la normativa a que se ha hecho referencia.

Por tanto, a la vista de lo anteriormente señalado, con independencia del tipo de dato personal de que se trate, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley Orgánica, recabándose, en caso de menores de catorce años cuyas condiciones de madurez no garanticen la plena comprensión por los mismos del consentimiento prestado, el consentimiento de sus representantes legales.

Ello no obstante, debe añadirse que si el tratamiento de los datos llevara aparejada algún tipo de disposición patrimonial por parte del menor, será necesario considerar que si bien se ha indicado que el menor de edad posee plena capacidad para consentir el tratamiento de sus datos personales, aquél carecerá de la suficiente capacidad para la realización de la citada disposición. Debe, en este sentido, recordarse que, según se desprende del texto del artículo 1261 del Código Civil, no

hay contrato sin el consentimiento de los contratantes, siendo el consentimiento el concurso de la oferta y aceptación sobre la cosa y causa que han de constituir el contrato, según el artículo 1262, y previniendo el artículo 1263 que no pueden prestar consentimiento los menores no emancipados. Por tanto, en este supuesto, será preciso no sólo el consentimiento del menor al tratamiento de sus datos, sino que deberá concurrir al mismo su representante legal.

II

Asimismo, la consultante se refiere a la posibilidad de ceder los datos académicos de los menores a sus padres o tutores sin el consentimiento de aquéllos. Además, se plantea -en concreto- si debe prevalecer la voluntad de un alumno de catorce años que no quiera que se faciliten sus calificaciones académicas a sus padres o tutores, sobre la pretensión de éstos de acceder a dicha información, no pudiendo en dicho caso el colegio atender dicha solicitud de los padres o tutores.

En cuanto a la posibilidad de ceder los datos académicos de los menores a sus padres o tutores sin el consentimiento de dichos menores afectados, ante todo, deberá considerarse que la comunicación de los datos al representante legal supone una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley como "Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado."

Respecto de las cesiones, el artículo 11.1 prevé taxativamente que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado." Este consentimiento sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2 de la Ley, entre los que se encuentra la posibilidad de que una norma con rango de Ley habilite la cesión.

Pues bien, de acuerdo con lo dispuesto por el artículo 154 del vigente Código Civil:

"Los hijos no emancipados están bajo la potestad del padre y de la madre.

La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y comprende los siguientes deberes y facultades:

1. Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.

2. Representarlos y administrar sus bienes (.....)".

En consecuencia, toda vez que la facultad de acceder a la información de carácter académico a la que se refiere la consultante (entre la que se cita la cesión relativa a las calificaciones obtenidas por los menores), se encuentra dentro del marco de los deberes y derechos que corresponden a los padres, inherentes al ejercicio de su patria potestad, cabe concluir que en el supuesto de los hijos no emancipados existe una norma legal habilitante que ampara la cesión de los datos académicos de los menores a sus padres, derivada de lo previsto en el transcrito artículo 154 del Código Civil.

De otra parte, en lo que a los tutores se refiere, idéntica previsión, constitutiva de la habilitación legal exigida por el artículo 11.2 a) de la Ley Orgánica de Protección de Datos, se encuentra en lo dispuesto por el artículo 269 del meritado Código Civil, cuando dispone que:

"El tutor está obligado a velar por el tutelado y, en particular:

1. A procurarle alimentos.

2. A educar al menor y procurarle una formación integral.

3. A promover la adquisición o recuperación de la capacidad del tutelado y su mejor inserción en la sociedad.

4. A informar al Juez anualmente sobre la situación del menor o incapacitado y rendirle cuenta anual de su administración."

En consonancia con dicho precepto, para los tutores se obtienen similares consecuencias que las expuestas más arriba para los padres que ejercen la patria

potestad, por lo que la cesión de los datos a que se refiere el consultante resultará conforme con lo previsto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

III

Asimismo, la consulta plantea si, en el supuesto de un colegio privado, y dado que existe una relación contractual entre el colegio y los padres que no puede ser asumida por el menor, sería lícito facilitar dichas calificaciones como resultado de los servicios contratados. Además, la consulta plantea si en el supuesto de que el alumno tuviera problemas de adaptación en el colegio, el hecho de comunicarlo a sus padres podría ser constitutivo de infracción, conllevando la correspondiente sanción, de acuerdo con lo dispuesto en la Ley Orgánica de Protección de Datos. Igualmente, la consultante plantea idéntica cuestión en el supuesto de que los datos sean solicitados por los servicios sociales de una Comunidad Autónoma que actúe como tutor del menor.

En relación con la primera de las cuestiones planteadas, la consultante apunta la posible aplicación de lo previsto por el artículo 11.2 c) de la Ley Orgánica 15/1999, cuando dispone que "el consentimiento exigido en el apartado anterior no será preciso ... Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique".

Pues bien, a nuestro juicio, dicho precepto no resulta aplicable al supuesto planteado, debiendo traerse a colación idéntica argumentación jurídica que la expuesta en el Punto II de este informe.

En consecuencia, con independencia del tipo de Centro Escolar de que se trate (público o privado) y, en su caso, de la existencia de una relación contractual entre dicho Centro y los padres o tutores del menor, la cesión de los datos relativos a las calificaciones académicas de éste, así como la comunicación de cualquier circunstancia relativa a la adaptación o inadaptación del menor al Centro Escolar, se encontrará amparada legalmente por los transcritos artículos 154 y 269 del vigente Código Civil.

Igualmente, en el supuesto de que los datos sean solicitados por los servicios sociales de una Comunidad Autónoma que actúe como tutor del menor, resultará aplicable la habilitación legal contenida en el artículo 269 del tan citado Código Civil, sin perjuicio de la existencia de otras normas de ámbito estatal y autonómico que ofrezcan idéntica cobertura en atención a las funciones legalmente conferidas a dichas Comunidades Autónomas cuando actúan en su condición de tutores del menor.

IV

Por último, se plantea si en el caso de los menores, el ejercicio de sus derechos de acceso, rectificación y cancelación, requerirá en todo caso de la concurrencia de la autorización de sus padres o tutores o, por el contrario, será suficiente atender a la edad del menor válida para la recogida de los datos, sin exigir en este supuesto complemento alguno de la capacidad del menor.

Pues bien, de acuerdo con lo dispuesto por el artículo 30 de la vigente Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en consonancia con lo expuesto en los apartados precedentes de este Informe, "Tendrán capacidad de obrar ante las Administraciones Públicas, además de las personas que la ostenten con arreglo a las normas civiles, los menores de edad para el ejercicio y defensa de aquellos de sus derechos e intereses cuya actuación esté permitida por el ordenamiento jurídico-administrativo sin la asistencia de la persona que ejerza la patria potestad, tutela o curatela. Se exceptúa el supuesto de los menores incapacitados, cuando la extensión de la incapacitación afecte al ejercicio y defensa de los derechos o intereses de que se trate".

De lo anterior se extrae que los menores de edad a los que, según se expone en el Punto I de este Informe, no se exija complemento alguno de su capacidad en orden a la recogida de sus datos de carácter personal, podrán ejercitar sus derechos de acceso, rectificación y cancelación, sin la concurrencia de la autorización de sus padres o tutores.

Informe 0501/2005 sobre: La naturaleza de los ficheros de un Colegio Privado Concertado.

La consulta plantea si, de acuerdo con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, un Colegio Público Concertado debe proceder a la notificación de sus ficheros, a fin de lograr su inscripción en el Registro General de Protección de Datos, a través del modelo de notificación de tratamiento de datos de carácter personal de titularidad pública o privada.

I

Con carácter previo, y sin ánimo de prejuzgar los términos de la solicitud de Informe a la que el escrito del consultante se refiere, parece deducirse que la inscripción de que se trata se refiere a un "Colegio Privado Concertado", y no a un "Colegio Público Concertado", por cuanto el régimen de Concierto con los Centros Educativos se vincula ex lege a personas jurídico-privadas.

Como punto de partida, el artículo 5 del Real Decreto 1332/1994, de 20 de junio, declarado vigente por la Disposición transitoria tercera de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, establece que "Todo fichero de datos de carácter personal, de titularidad pública, será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia, de una copia de la disposición de creación del fichero".

En consecuencia, la obligación de notificación corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

II

Para determinar a quién corresponde la obligación de proceder a la adopción de la correspondiente disposición de carácter general y la consiguiente notificación del tratamiento al Registro General del Protección de Datos resulta imprescindible delimitar si el consultante es un órgano incardinado en la Administración Autonómica o si el mismo posee personalidad jurídica independiente de la misma.

En el primer supuesto, el Centro no sería sino un mero usuario del fichero, cuyo responsable sería la Administración educativa autonómica, de forma que la obligación de notificación correspondería a la Consejería de Educación de la Comunidad Autónoma correspondiente, debiendo hacerse referencia al Centro educativo únicamente como lugar de ubicación del fichero. En caso contrario, el responsable del fichero sería el propio Centro,
correspondiendo al mismo la notificación del tratamiento al Registro de esta Agencia.

Según dispone el artículo 64 de la Ley Orgánica 10/2002, de Calidad de la Educación "Los centros docentes se clasifican en públicos y privados", añadiendo que "Son centros públicos aquellos cuyo titular sea un poder público".

En consecuencia, dicha Ley Orgánica vincula el carácter público de los Centros con la titularidad de los mismos. Al propio tiempo, la misma no establece en ningún lugar si los centros tendrán o no personalidad jurídica dependiente de la correspondiente Administración Educativa, si bien especifican expresamente los ámbitos en que los mismos gozarán de autonomía pedagógica, organizativa y de gestión económica (artículos 67 a 70 de la Ley Orgánica).

Por su parte, las diferentes normas de las Comunidades Autónomas reguladoras de la enseñanza no universitaria establecen únicamente el carácter público de los Centros de Enseñanza Públicos, por lo que, a sensu contrario, el resto de los Centros de

Enseñanza, que no son de titularidad pública, han de reputarse como Centros Privados.

De lo dispuesto en la legislación básica estatal y en la autonómica a la que acaba de hacerse referencia se desprende que los Centros Públicos de Enseñanza no son sino órganos directamente dependientes de la Consejería autonómica correspondiente y carentes de personalidad propia y diferenciada de la misma, sin prejuicio de las peculiaridades que les son propias en lo referente al respeto de los principios de autonomía pedagógica, organizativa y de gestión económica que la Ley establece.

Por ello, ha de concluirse que, cuando los Centros Educativos de Enseñanza se encuentren integrados orgánicamente en la Administración autonómica, será ésta la obligada al cumplimiento de las obligaciones que respecto de los ficheros de titularidad pública impone la Ley Orgánica 15/1999, debiendo la misma adoptar la correspondiente disposición de carácter general y proceder a la notificación de los tratamientos al Registro General de Protección de Datos, en la que se hará constar que el Centro es el lugar de ubicación del fichero.

Por el contrario, en el resto de los casos, como ocurre en el supuesto sometido a consulta, en el que se plantea la inscripción de la notificación de ficheros de un Colegio Privado Concertado, el responsable del fichero será el propio Centro, correspondiendo al mismo la notificación del tratamiento al Registro General de Protección de Datos de esta Agencia, utilizando a tal fin el modelo de notificación de tratamiento de datos de carácter personal de titularidad privada, de acuerdo con lo dispuesto por el artículo 26 de la Ley Orgánica 15/1999.

Informe 37/2006 sobre: La cesión de datos de evaluación de profesorado.

La consulta plantea si procede la cesión de datos referentes a los resultados de encuestas anónimas de evaluación del profesorado a los órganos encargados de velar por la calidad y el adecuado desarrollo de las enseñanzas impartidas en la Universidad, haciendo expresa referencia a las comisiones establecidas por el artículo 53 de los estatutos de la propia Universidad y, en particular, a las Comisiones de Docencia y las Comisiones de Calidad de la Docencia, si bien las mismas no han sido constituidas como tales, según indica la consulta.

Como cuestión previa, deben efectuarse determinadas consideraciones relativas al sometimiento del tratamiento al que se refiere la consulta a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

En este sentido, el artículo 2.1, párrafo primero de la Ley dispone que "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", siendo datos de carácter personal "Cualquier información concerniente a personas físicas identificadas o identificables", tal y como dispone el artículo 3 a).

En el presente caso, con independencia de que no sean conocidos los datos de quienes dan respuesta a las encuestas no cabe duda que nos encontraremos ante datos de carácter personal referidos al profesorado respecto del que se efectúa la encuesta, toda vez que se vincularán los resultados de la evaluación a cada afectado concreto objeto de aquélla.

En consecuencia, el tratamiento de los datos quedará sometido a lo dispuesto en la Ley Orgánica 15/1999, debiendo indicar que, en lo referente a la exactitud de los datos, consagrada por el artículo 4.3 de la Ley Orgánica, la misma existirá siempre que los datos correspondan a la valoración efectivamente realizada, dado que en ese punto ha de considerarse que concluiría la responsabilidad de quien trata los datos, sin perjuicio de la fiabilidad que hubiera de otorgarse a los resultados de la encuesta en virtud del carácter más o menos técnico de las cuestiones planteadas y los conocimientos del alumnado que responde al cuestionario de evaluación.

Respecto de la comunicación de los datos a distintos órganos universitarios, la propia consulta recuerda la opinión de estas Agencia, manifestada en su informe de 21 de diciembre de 2005, emitido a instancia del Defensor Universitario, en que se señala que la transmisión de los datos, sometidos como se ha dicho a lo dispuesto en la Ley Orgánica 15/1999, supondrá una cesión o comunicación de datos.

Respecto de la misma ya se indicó que se encontrarían amparadas en lo dispuesto en la Ley Orgánica 6/2003, en conexión con lo previsto en los Estatutos de la Universidad, las cesiones que la consulta planteaba, siendo ahora preciso aclarar la consulta en cuanto a qué órganos deberían ser destinatario concretos de los datos en cada caso.

El artículo 4.1 de la Ley Orgánica 15/1999 dispone que "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

En consecuencia, el tratamiento devendrá lícito cuando el mismo corresponda al cumplimiento de las finalidades legítimamente predicables de quiene procede a dicho tratamiento. En este mismo sentido, el primer inciso del artículo 11.1 de la Ley Orgánica 15/1999 dispone que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario".

En el ámbito de las Administraciones Públicas y de los organismos vinculados o dependientes de las mismas la materialización del principio de finalidad se verifica a

través del principio de competencia, de modo que podrán ser tratados los datos por quien legítimamente tenga la competencia para proceder a ese tratamiento y siempre respetando los restantes principios contenidos en la legislación vigente en materia de protección de datos de carácter personal.
Precisamente por ese motivo, el artículo 21.1 de la Ley Orgánica 15/1999, interpretado a sensu contrario, habilita la cesión de datos entre Administraciones Públicas cuando la cesión se realice en el ejercicio de una misma competencia.
Pues bien, completando lo indicado en el informe de esta Agencia de 21 de diciembre de 2001, el destinatario de los datos en cada caso habrá de ser el órgano al que se encomiende en cada supuesto el control del adecuado desarrollo de las actividades formativas dentro de las Facultades, Escuelas y, dentro de las mismas, Departamentos, del Centro Universitario.
De los preceptos de los Estatutos transcritos en la consulta no se desprende de modo unívoco que las Comisiones a las que la misma se refiere tengan atribuidas competencias tales que permitan considerar legítimo el tratamiento de los datos resultantes de las evaluaciones, por lo que, a la vista de dichos preceptos, la comunicación de los datos a dichas comisiones no se encontraría amparada por lo dispuesto en la Ley Orgánica 15/1999.

Informe 227/2006 sobre: El acceso a datos escolares por padres y familiares.

La consulta plantea determinadas cuestiones relacionadas con el acceso a la información de los alumnos que es objeto de tratamiento por parte del centro consultante, conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

II

Antes de entrar a analizar las cuestiones planteadas conviene señalar que los datos mencionados en la consulta se encuentran, en todo caso, sometidos a lo dispuesto en la Ley Orgánica 15/1999, ya que la misma define en su artículo 3 a) los datos de carácter personal como "Cualquier información concerniente a personas físicas identificadas o identificables".

No obstante, es preciso señalar que los citados datos podrán referirse no sólo a los propios alumnos del centro, sino a terceras personas distintas de aquéllos. Así sucedería por ejemplo en lo referente a los datos económicos citados en la consulta, dado que los conceptos facturados podrán referirse al alumno, si bien los datos referidos al efectivo abono de los servicios prestados por el centro podrán referirse al padre o madre que efectivamente procedan a su pago. Esta consideración deberá ser tenida especialmente en cuenta en relación con el ejercicio de los derechos de acceso y con otra serie de cuestiones que se analizarán en un momento posterior.

Por otra parte, deberían diferenciarse los supuestos en que la información es facilitada a la persona a la que aparecen referidos los datos, esto es, al afectado, en los términos definidos en el artículo 3 e) de la Ley Orgánica 15/1999 de aquellos otros en los que el destinatario de la información no es el propio afectado.

En el primero de los supuestos podremos encontrarnos ante un supuesto de ejercicio del derecho de acceso, al que se refiere el artículo 15 de la Ley Orgánica 15/1999, cuyo apartado primero establece que "El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos".

Por su parte, en caso de que el destinatario de los datos no sea el propio afectado nos encontraremos ante una cesión de datos de carácter personal, definida en el artículo 3 i) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado".

Respecto de las cesiones, el artículo 11.1 de la Ley Orgánica 15/1999 dispone que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". No obstante sería posible la cesión sin contar con el consentimiento del interesado en los supuestos contemplados en el artículo 11.2 de la propia Ley.

Por su parte, debe también tenerse en cuenta que algunos de los datos a los que se refiere la consulta se encuentran relacionados con la salud del afectado y, por tanto, tienen la condición de datos especialmente protegidos. Por este motivo, deberá tenerse en cuenta lo dispuesto en el artículo 7.3, según el cual "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

Dicho todo lo anterior, procederá ahora dar respuesta a las cuestiones planteadas.

III

La primera de las cuestiones se refiere a la posibilidad de que los datos mencionados en la consulta puedan ser facilitados a los propio alumnos del centro, aún cuando los mismos sean menores de edad.

En este caso, en lo que se refiera a dato relacionados con el alumno nos encontraremos, como ya se ha dicho ante una forma de ejercicio del derecho de

acceso, siendo necesario analizar si dicho derecho podrá ser ejercitado directamente por el menor o si sería precisa la asistencia de su representante legal.
La cuestión planteada ha sido objeto de informe por parte de esta Agencia en reiteradas ocasiones. Si bien la doctrina manifestada en dichos informes venía referida a la posibilidad de que el menor pudiera consentir por sí mismo el tratamiento de sus datos de carácter personal ha de ser igualmente aplicada a los supuestos de ejercicio del derecho de acceso por parte de los menores de edad.
Así, en informe de esta Agencia de 8 de abril de 2004 se indicaba lo siguiente:
"A nuestro juicio, deben diferenciarse dos supuestos básicos, el primero referido a los mayores de 14 años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el segundo, al consentimiento que pudieran prestar los menores de dicha edad.
Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".
Se plantea entonces si, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 para los mayores de catorce años.
Por otra parte, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en Resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.
En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal.
Respecto de los restantes menores de edad, no puede ofrecerse una solución claramente favorable a la posibilidad de que por los mismos pueda prestarse el consentimiento al tratamiento, por lo que la referencia deberá buscarse en el artículo 162 1º del Código Civil, tomando en cuenta, fundamentalmente, sus condiciones de madurez."
La doctrina contenida en el citado informe es, como se ha indicado, extrapolable al supuesto ahora analizado, dado que el ejercicio del derecho de acceso es una manifestación de un acto referido a derechos de la personalidad. Por tanto, si el menor tuviese más de catorce años será posible facilitarle la información solicitada. En caso

contrario habrían de ser atendidas sus condiciones de madurez en atención a los datos que sería objeto de transmisión al mismo.
En todo caso, la transmisión al alumno de los datos debería limitarse a aquellos que se refieran al mismo, dado que en caso contrario se produciría una cesión o comunicación de datos de carácter personal, sin que la misma pueda considerarse amparada en ninguno de los supuestos contemplados en el artículo 11.2 de la Ley Orgánica 15/1999.

IV

El resto de las cuestiones planteadas se refiere a la posibilidad de entrega de los datos referidos en la consulta a los padres del menor, así como a otros familiares, planteándose asimismo si es posible la comunicación de los datos a quien no es "titular de la solicitud de matrícula y que hace efectivos los recibos mensuales".
Como ya se indicó con anterioridad, en el supuesto planteado nos encontraremos, con carácter general, ante una cesión o comunicación de datos de carácter personal, que deberá cumplir lo establecido en el artículo 11 o, en caso de datos de salud, en el artículo 7.3 de la Ley Orgánica 15/1999.
Dicho esto, el artículo 154 del Código Civil dispone que "Los hijos no emancipados están bajo la potestad del padre y de la madre", añadiendo que "La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y comprende los siguientes deberes y facultades (...) Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral".
En consecuencia, en lo que se refiere a los datos que guarden relación con las funciones de educación y formación establecidas en el citado artículo 154 del Código Civil, existe una norma con rango de Ley que habilita la cesión o comunicación de datos de carácter personal, por lo que la cesión de los datos académicos o psicopedagógicos que guarden directa relación con esos deberes formativos se encontraría amparada en el artículo 11.2 a) de la Ley Orgánica 15/1999 en relación con el artículo 154 del Código Civil.
Al propio tiempo, el artículo 159 del Código Civil establece que "si los padres viven separados y no decidieren de común acuerdo, el Juez decidirá, siempre en beneficio de los hijos, al cuidado de qué progenitor quedarán los hijos menores de edad".
De este modo, en tanto no exista una resolución judicial que excluya del ejercicio de la patria potestad a uno de los progenitores no será posible considerar inaplicable la habilitación que venimos estudiando, por lo que el progenitor seguiría encontrándose habilitado para que le fuesen cedidos los datos.
Por otra parte, como se ha venido indicando, la habilitación se refiere a los titulares de la patria potestad y no a cualesquiera familiares, que únicamente podrían obtener los datos en caso de ejercer la tutela, dado que el artículo 269 del Código Civil establece una habilitación legal similar, al disponer que "El tutor está obligado a velar por el tutelado y, en particular (...) a educar al menor y procurarle una formación integral".
En consecuencia, en relación con los datos relacionados directamente con la educación y formación del menor, y en respuesta a las cuestiones planteadas, debe concluirse que será posible la cesión a cualquiera de los progenitores mientras ejerzan la patria potestad, no pudiendo en ese caso denegarse la cesión por el hecho de que exista separación en tanto no se haya adjudicado la patria potestad en exclusiva a uno de os progenitores. Al propio tiempo, los restantes familiares únicamente podrían acceder a los datos en caso de ostentar la tutela del menor.

V

En cuanto a los restantes datos mencionados en la consulta, no sería aplicable la excepción planteada.
En particular, en relación con los datos de salud, el acceso a los mismos debería regirse, a sensu contrario, por lo expuesto en el apartado II del presente informe, de forma que en caso de que el menor fuera mayor de catorce años el acceso

únicamente sería posible si fuese solicitado por el menor o aquél hubiese apoderado al progenitor para ello. Si el menor tuviese menos de catorce años debería estarse a sus condiciones de madurez. Así lo ha señalado la Agencia en informe de 29 de septiembre de 2004.

Informe 0262-2006 sobre: Videovigilancia en los colegios

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta formulada por, cúmpleme informarle lo siguiente:
La consulta plantea dudas sobre si la instalación de una cámara de videovigilancia en centros educativos para controlar casos de violencia, acoso escolar y actos vandálicos como robos y daños materiales resulta una medida proporcionada y justificada, de conformidad con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y los requisitos que deberían observarse para la instalación de las citadas cámaras.
Con carácter general, la vigilancia por videocámaras puede estar justificada en determinadas circunstancias, sin embargo se hace necesario adecuar la videovigilancia a las exigencias del derecho fundamental a la protección de datos de manera que el tratamiento de imágenes con fines de videovigilancia sea adecuado a los principios de la Ley Orgánica 15/1999 y garantizar así los derechos de las personas cuyas imágenes son tratadas por medio de tales procedimientos.
En este sentido, todo uso de videocámaras, tanto en el ámbito escolar como en cualquier otro ámbito en los que se considere necesaria su instalación, debe respetar el principio de proporcionalidad, tanto en su vertiente de indoneidad (sólo pueden emplearse cuando resulte adecuado) como de intervención mínima (ponderación entre los fines pretendidos y la afectación a los derechos fundamentales de los ciudadanos).
Es por ello que la grabación de la imagen de una persona es un dato de carácter personal, siendo éste el criterio de la Agencia Española de Protección de Datos, tal y como ha quedado reflejado en los Fundamentos de Derecho de la Resolución R/00035/2006 de 27 de febrero de 2006, donde se estable que:
"El artículo 1 de la LOPD dispone: "La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala: "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como "Cualquier información concerniente a personas físicas identificadas o identificables".
El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.
De acuerdo con aquella definición de tratamiento de datos personales, la captación de imágenes de las personas que transitan una vía publica constituye un tratamiento de datos personales incluido en el ámbito de aplicación de la normativa citada.
El artículo 1.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, considera datos de carácter personal a "toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable".

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 personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal "toda información sobre una persona física identificada o identificable; 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". Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.
Atendiendo a la definición contenida en las normas citadas, que considera dato de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables", las grabaciones indicadas se ajustarán a este concepto siempre que permitan la identificación de las personas que aparecen en dichas imágenes. La Directiva 95/46/CE en su Considerando 14 lo afirma expresamente al señalar:
"(14)Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;".
Siguiendo con la Fundamentación Jurídica de la resolución que se cita y a efectos de valorar los criterios de proporcionalidad en relación con la instalación de este tipo de sistemas, dispone que:
"El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas. En relación al tratamiento de datos constituidos por imagen y sonido relativos a personas físicas, en dicho documento se declara la plena aplicabilidad de las disposiciones de la citada Directiva relativas a:
. Calidad de los datos: Las imágenes serán tratadas de manera leal y lícita, y se destinarán a fines determinados, explícitos y legítimos. Se utilizarán de conformidad con el principio según el cual los datos deberán ser adecuados, pertinentes y no excesivos, y no serán tratados posteriormente de manera incompatible con dichos fines; se conservarán durante un periodo limitado, etc.
. Principios relativos a la legitimación del tratamiento de datos: En base a estos principios, es necesario que el tratamiento de datos personales mediante vigilancia por videocámara esté fundamentado en al menos uno de los requisitos mencionados en el artículo 7 (consentimiento inequívoco, necesidad de obligaciones contractuales, de cumplimiento de una obligación jurídica, de protección de un interés vital del interesado, de cumplimiento de una misión de interés público o inherente al ejercicio del poder público, equilibrio de intereses, etc.).
. Tratamiento de categorías especiales de datos, sujeto a las garantías aplicables al uso de datos sensibles o datos relativos a infracciones en el marco de la vigilancia por videocámara (con arreglo al artículo 8).
. Información que se facilitará al interesado (artículos 10 y 11).
. Derechos del interesado, en concreto el derecho de acceso y el derecho de oposición al tratamiento por razones legítimas (artículo 12 y letra a) del artículo 14).

. Garantías aplicables en relación con las decisiones individuales automatizadas (artículo 15).
. Seguridad de las operaciones de tratamiento (artículo 17).
. Notificación de las operaciones de tratamiento (artículos 18 y 19).
. Controles previos de las operaciones de tratamiento que puedan presentar riesgos específicos para los derechos y libertades del interesado (artículo 20).
. Transferencia de datos a terceros países (artículo 25 y siguientes).

Por otra parte, para determinar si el supuesto que se analiza implican el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos.

En cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos se mencionan, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso....

Por tanto, la captación y grabación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, máxime cuando los afectados resultan perfectamente identificables, dentro del ámbito donde se realiza la captación de imágenes."

Además este es el criterio que se hace constar en la Instrucción 1/2006 de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras**,** que se publicó en el B.O.E de 12 de diciembre de 2006, pues así lo dispone su artículo uno en el que se señala que "La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras. El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas. Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados."

En relación con la instalación de sistemas de videocámaras, la Instrucción 1/2006 hace especial referencia a la necesidad de ponderar los bienes jurídicos protegidos. Así viene a señalar expresamente que la instalación de este tipo de dispositivos se deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

En consecuencia, la instalación de cámaras de videovigilancia en el supuesto de la consulta es decir en un centro escolar con el fin de controlar determinadas conductas violentas ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia, por lo que desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.

En cuanto a la proporcionalidad, tal y como señala la propia Instrucción, la Sentencia del Tribunal 207/1996 determina que se trata de "una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad".

Así, el artículo 4 de la Instrucción 1/2006 recoge los principios de calidad, proporcionalidad y finalidad del tratamiento estableciendo lo siguiente:

"1.- De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2.- Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3.- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida."

En este sentido, si la finalidad de la instalación de cámaras de videovigilancia tiene como objetivo el control de casos graves de violencia o acoso escolar en donde la propia integridad física de los alumnos pudiera correr peligro o de ello se derivaran graves consecuencias psicológicas, en principio, la medida podría considerarse idónea, necesaria y proporcional, siempre y cuando se limitase estrictamente a esa finalidad. No obstante lo anterior, sería necesario atender las circunstancias particulares de cada centro educativo.

Por otro lado, a la hora de regular la legitimación del tratamientos de imágenes, la Agencia Española de Protección de Datos, entiende que es requisito esencial la aplicación íntegra del artículo 6.1 y 2 y del artículo 11.1 y 2 de la LOPD, sin perjuicio del estricto cumplimiento de los requisitos que para la instalación de cámaras o videocámaras de vigilancia vengan exigidos por la legislación vigente (artículo 2 de la Instrucción).

Además, se hace necesario indicar, que el tratamiento de las imágenes por parte del responsable del tratamiento (en el supuesto de la consulta, los centros escolares), le obliga a cumplir con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la Ley Orgánica que dispone, "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la

negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".
En cuanto al modo en que haya de facilitarse dicha información, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006 cuando establece que "Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de La Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:
a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y
b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.
El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción."
Así mismo, deberán respetarse los plazos y procedimiento de almacenamiento de imágenes, resultando de aplicación, el artículo 6 de la mencionada Instrucción en la que se prevé que "los datos serán cancelados en el plazo máximo de un mes desde su captación" Respecto al procedimiento de grabación de imágenes deberá de cumplir con lo dispuesto en la Ley Orgánica 15/1999, para la recogida de datos, que como anteriormente hemos fijado, deberá de cumplirse con el deber de informar.
Atendiendo a lo que acabamos de indicar y en relación con las cuestiones que se plantean en el supuesto de la consulta, cabe extraer las siguientes conclusiones:
PRIMERA: La instalación de cámaras de videovigilancia sería una medida proporcional y justificada si se cumplen los siguientes requisitos:
1. Que se trate de una medida susceptible de conseguir el objetivo propuesto.
2. Que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
3. Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.
SEGUNDA: En todo caso, los responsables de este tipo de tratamientos deben ser plenamente conscientes del respeto a la protección de datos de carácter personal, resultando de aplicación las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como en sus respectivas normas de desarrollo y en especial la recientemente publicada Instrucción 1/1996 en lo que se refiere a su ámbito subjetivo de aplicación, la legitimación para su tratamiento, el contenido del deber de información , el respeto a los principios de calidad, proporcionalidad y finalidad de su tratamiento, así como el ejercicio de los derechos a que se refieren los artículos 15 y siguientes de la citada Ley Orgánica. Además, la creación de un fichero de videovigilancia exige su previa notificación a la Agencia Española de Protección de Datos, para la inscripción en su Registro General y el cumplimiento del deber de seguridad y secreto respecto a su tratamiento en los términos previstos en la Ley 15/1999 y en su reglamento de desarrollo.

Informe 368/2006 sobre: La proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio.

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por XXX, cúmpleme informarle lo siguiente:
La consulta plantea si, de acuerdo con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, el consultante puede establecer un sistema de control para gestionar las ausencias y retrasos de los alumnos, basado en la obtención de la huella dactilar de éstos.
Mediante dicha huella dactilar pretende controlarse la entrada y salida de los alumnos en el centro escolar.
Para resolver la cuestión planteada debe partirse del análisis de la incidencia que los datos biométricos tienen en el ámbito de aplicación de la citada Ley Orgánica 15/1999, de 13 de diciembre.
Son datos biométricos aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto de dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión. Así se emplean para tales fines las huellas digitales, el iris del ojo, la voz, etc.
Por su parte, el artículo 3 a) de la Ley Orgánica de Protección de Datos define los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificables". En este sentido debe indicarse que, si bien el procesamiento de los datos biométricos no revela nuevas características referentes al comportamiento de las personas sí permite, lógicamente, su identificación, por lo que resulta evidente que, en caso de procederse a su tratamiento dicho tratamiento deberá ajustarse a la Ley Orgánica 15/1999.
Según el artículo 4.1 de la Ley Orgánica, sólo se podrán recoger datos de carácter personal para su tratamiento, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. El problema se planteará entonces en determinar si el tratamiento de la información biométrica de huella dactilar puede ser considerado excesivo para el fin que motiva dicho tratamiento, teniendo en cuenta que se efectuaría un tratamiento de datos de menores de edad para las finalidades a las que nos hemos referido al comienzo del presente informe.
A nuestro juicio, tal y como se ha venido indicando por el Grupo de trabajo creado por el artículo 29 de la Directiva 95/46/CE, en el Documento de Trabajo sobre biometría, de fecha 1 agosto de 2003, la obtención de la huella dactilar como medio para identificar a los alumnos en el centro resulta excesivo y desproporcionado, para dicha finalidad.
"Con arreglo al artículo 6 de la Directiva 95/46/CE, los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. Además, los datos personales serán adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente (principio de fines).El cumplimiento de este principio implica en primer lugar una determinación clara de los fines para los que se recogen y tratan los datos biométricos.
Por otra parte, hace falta evaluar el cumplimiento de la proporcionalidad y de la legitimidad, teniendo en cuenta los riesgos para la protección de los derechos y libertades fundamentales de las personas y especialmente si los fines perseguidos pueden alcanzarse o no de una manera menos intrusiva.

La proporcionalidad ha sido el criterio principal en casi todas las decisiones adoptadas hasta ahora por las autoridades encargadas de la protección de datos sobre el tratamiento de datos biométrico....
El uso de la biometría plantea también el tema de la proporcionalidad de cada categoría de datos a la luz de los fines para los que se tratan dichos datos. Los datos biométricos sólo pueden usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados. Por ejemplo, la CNIL francesa ha rechazado el uso de huellas digitales en el caso del acceso de los niños a un comedor escolar19, pero ha aceptado con el mismo fin el uso de los resultados de muestras de las manos. La autoridad portuguesa de protección de datos ha tomado recientemente una decisión desfavorable sobre la utilización de un sistema biométrico (huellas digitales) por parte de una universidad para controlar la asiduidad y puntualidad del personal no docente."
En consecuencia, entendemos que resulta desproporcionado y por ello contrario a lo dispuesto en el artículo 4.1 de la Ley Orgánica 15/1999 antes citado, la utilización de la huella dactilar como medio para controlar el acceso de los alumnos al centro escolar y tal finalidad puede conseguirse, sin duda, de una manera menos intrusiva en relación con los derechos de los alumnos.

Informe 0063-2008 sobre: La inclusión de datos en el sistema Seneca

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, cúmpleme informarle lo siguiente:

I

La consulta informa a esta Agencia acerca de la existencia del Programa SÉNECA, incorporando una breve descripción del mismo y señalando que su finalidad, según la Junta de Andalucía, consiste en "rentabilizar la información del alumnado, ya que cuando un alumno es registrado en el Programa SÉNECA al haber presentado una solicitud de admisión a algún centro de enseñanza sus datos son accesibles para cualquier centro de la Comunidad Autónoma sin que tenga que volver a registrarlo".

Asimismo, se indica que el programa implica la inclusión de datos relativos a la salud del alumno, en caso de que padezca algún tipo de incapacidad, o "las sanciones que se imponen desde el centro por la infracción de normas de convivencia", recordando que en este caso los datos se encuentran sometidos a las medidas de seguridad de nivel medio o alto. En particular, se indica que los datos son objeto de tratamiento sin contar con el consentimiento de los afectados.

Así, se plantea si los centros concertados se encuentran obligados a consignar los datos de los alumnos en el Programa, al carecer de consentimiento del interesado, señalando que desde la introducción de los datos "el centro recaudador pierde todo control sobre esos datos, toda vez que cualquier persona que tenga acceso al programa a través de una clave conociendo el nombre y apellidos de un trabajador o de un alumno de cualquier centro de Andalucía puede conocer sus datos personales".

Asimismo, se plantea si los centros incurrirían en infracción de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, como consecuencia de la introducción de los datos y, en resumen, si es posible que los centros concertados puedan negarse a la introducción de los citados datos.

II

La Orden de 20 de julio de 2006, de la Consejería de Educación de Andalucía, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de los sistema SÉNECA y PASEN, señala en su Anexo I que dichos sistemas "proporcionan la infraestructura técnica para el manejo de la información académica y de gestión de los centros educativos dependientes de la Consejería de Educación de la Junta de Andalucía", añadiendo que "esto incluye a los centros educativos de carácter público de la Comunidad y a los centros educativos concertados que utilizan estos sistemas para el soporte de determinados procesos de gestión".

En consecuencia, debe diferenciarse entre los ficheros de datos regulados por la citada Orden y los propios sistemas SÉNECA y PASEN, definidos por el propio texto como herramientas de manejo de la información y gestión académica de los centros integrados en el sistema educativo público de la Comunidad Autónoma.

En este sentido, el artículo 3.1 de la Ley 17/2007, de 10 de diciembre, de Educación de Andalucía establece que "el Sistema Educativo Público de Andalucía es el conjunto de centros, servicios, programas y actividades de las administraciones públicas de la Comunidad Autónoma o vinculados a las mismas, orientados a garantizar el derecho de la ciudadanía a una educación permanente y de carácter compensatorio, reconocido en el artículo 21.1 del Estatuto de Autonomía para Andalucía", añadiendo el apartado 3 que el Sistema está compuesto por los centros docentes públicos de titularidad de la Junta de Andalucía o de las Corporaciones Locales u otras Administraciones Públicas, así como por los centros docentes privados concertados, sin perjuicio de la legislación específica que pudiera resultar de aplicación a los mismos.

Dentro del ámbito competencial de la mencionada Comunidad Autónoma, la Ley 17/2007 contiene en su Título V determinadas previsiones tendentes a uniformar la gestión de los procesos automatizados de datos por parte de los centros integrados en el Sistema Público.

Así, el artículo 142.1 dispone que "la Administración educativa favorecerá el funcionamiento en red de los centros educativos, con objeto de compartir recursos, experiencias e iniciativas y desarrollar programas de intercambio de alumnado y profesorado".

Por su parte, conforme al artículo 151 "La Administración educativa facilitará e impulsará la realización de trámites administrativos a través de Internet, así como la relación electrónica de la ciudadanía con los centros docentes. A tales efectos, se prestará especial atención a los procedimientos de escolarización y matriculación del alumnado, así como a los que realizan los miembros de la comunidad educativa, particularmente el profesorado".

De lo dispuesto en la Orden de creación de ficheros y la Ley 17/2007 se desprende, como se ha venido indicando que los sistemas SÉNECA y PASEN se configuran como herramientas encaminadas a facilitar y agilizar los trámites relacionados con la gestión de los centros integrados en el Sistema Educativo Público de Andalucía, debiendo en consecuencia diferenciarse entre el propio sistema, como aplicación puesta a disposición de los Centros por la Administración Autonómica, en desarrollo de los artículos 142.1 y 151 de la Ley, de los propios ficheros previstos en la Orden o aquellos de los que en uso de la aplicación sean creados y gestionados por los centros integrados en el sistema.

De este modo, la situación es en principio similar a la de los sistemas de información existentes en otras áreas de actividad cuya competencia corresponda al sector público. Así, en principio, no cabría apreciar diferencia entre los sistemas analizados y otros que fueran desarrollados, por ejemplo, para la gestión de las historias clínicas en el ámbito del Sistema sanitario de una determinada Comunidad Autónoma o los que fueran desarrollados por un determinado departamento para la gestión de recursos humanos o la gestión presupuestaria de los restantes Departamentos integrantes de dicha Administración.

Consecuencia de lo que acaba de indicarse es que los Centros concertados, dotados de personalidad enteramente independiente de la Administración educativa autonómica serán responsables de los ficheros relacionados con la utilización de la herramienta o sistema informático puesto a su disposición, siendo tales ficheros diferentes de los creados expresamente para el ámbito de la Administración Pública por su propia Orden de creación.

III

Dicho lo anterior, y centrándonos ya en el tratamiento de datos llevado a cabo por los Centros concertados, a los que se ciñe la consulta, dicho tratamiento deberá encontrarse amparado por lo dispuesto en el artículo 6.1 de la Ley Orgánica 15/1999, según el cual "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".

Añade el artículo 6.2 que "no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se

comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".
Al propio tiempo, la transmisión de datos, incluso a través de los sistemas SÉNECA y PASEN a los que se refiere la consulta, desde el Centro concertado a la Administración educativa autonómica o a otros usuarios del sistema no integrados en la misma, a los que se refiere la consulta, constituirán cesiones de datos de carácter personal, definidas por el artículo 3 i) de la Ley Orgánica 15/1999 como "Toda revelación de datos realizada a una persona distinta del interesado".
En relación con las cesiones, el artículo 11.1 de la Ley indica que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". No obstante, este consentimiento no será preciso en caso de concurrir alguno de los supuestos previstos en el artículo 11.2 y, en particular, cuando la cesión se encuentre amparada por una norma con rango de Ley.
En particular, en relación con esta excepción, debe tenerse en cuenta que el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, prevé que dicha habilitación, además de en los supuestos de mención expresa, podrá entenderse producida, en particular, cuando:
- El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.
- El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

Por otra parte, si se tratase de datos relacionados con la salud de los alumnos, el artículo 7.3 de la Ley Orgánica 15/1999 dispone que "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente". Por tanto, deberá existir una habilitación legal para el tratamiento y cesión de estos datos, interpretada en los términos contenidos en el Reglamento, a los que acaba de hacerse referencia.
En consecuencia, la existencia de los sistemas SÉNECA y PASEN e incluso la exigencia de su uso por la Administración educativa autonómica no implican necesariamente una habilitación genérica para el tratamiento de los datos por parte del personal del centro concertado ni tampoco el acceso a la información sometida a tratamiento por parte de usuarios del sistema no integrados en el centro. Dichos tratamiento y acceso deberán encontrarse, además, amparados en una de las causas establecidas en los artículo 6 y 11 de la Ley Orgánica 15/1999 a los que se ha hecho referencia.

IV

En cuanto al tratamiento de datos de los alumnos o del personal del Centro por parte del mismo, la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, dispone en sus tres primeros apartados, lo siguiente:
"1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.
2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un

centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo."

En consecuencia, el tratamiento de los datos por el Centro se encontrará amparado en lo establecido en la mencionada Disposición adicional, siempre que los datos aparezcan vinculados a las finalidades descritas detalladamente en el apartado 1 de la misma.

De este modo, será en todo caso posible el tratamiento por los Centros de los datos identificativos de los alumnos, así como de sus circunstancias personales o familiares, los relacionados con el desarrollo de su escolarización, como podrían ser los vinculados a la imposición de sanciones disciplinarias por cualesquiera conductas, incluidas las contrarias al deber de convivencia impuesto al alumno por la Ley Orgánica 8/1985, de 3 de julio, reguladora del derecho a la educación, los correspondientes a la escolarización y evaluación de los alumnos, así como los necesarios para la adecuada educación y orientación de aquéllos, no siendo preciso el consentimiento de los alumnos o sus padres o tutores para el tratamiento de dichos datos.

V

En cuanto a las cesiones, ya se ha venido indicando que las mismas habrán de tener cobertura en lo dispuesto en la Ley, comprendiendo esta habilitación tanto a la Ley Orgánica 2/2006 como a la Ley 12/2007, a las que ya se ha hecho referencia con anterioridad.

De este modo, las mencionadas normas deberán prever conforme a las habilitaciones a las que se ha hecho referencia competencias o previsiones especiales habilitantes de la cesión, dado que el apartado 4 de la Disposición adicional vigésimo tercera de la Ley Orgánica 2/2006 dispone expresamente que "la cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal, y las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas en el seno de la Conferencia Sectorial de Educación".

Por otra parte, la cesión de datos a otros centros integrantes del sistema educativo autonómico y distintos de los órganos educativos se encuentra prevista en el apartado 2 de la citada Disposición adicional, según el cual "la incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos". No obstante, es preciso recordar que el precepto añade que "en todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso".

De este modo, la cesión aparece vinculada con la legitimación que el centro de destino podrá tener ara el tratamiento de los datos de los alumnos, conforme a lo establecido en el apartado 1 de la disposición adicional al que se ha hecho referencia en el apartado anterior de este informe.

De lo que acaba de indicarse, cabrá extraer dos consecuencias en relación con el acceso a los datos que hayan sido objeto de tratamiento a través de los sistemas o aplicaciones SÉNECA y PASEN:
- El acceso a los datos por parte de la Administración educativa, estatal o autonómica deberá encontrase amparado por lo dispuesto en las Leyes estatal o autonómica en materia de educación.
- El acceso por usuarios de otros centros sólo será posible en caso de que se refiera a los datos de alumnos de ese centro, procedentes de otro centro distinto y exclusivamente en cuanto a los datos estrictamente necesarios para el desarrollo de la función docente y educativa.

VI

Dado que los accesos habilitados por la Ley Orgánica 15/1999 se deberán circunscribir a los que acaban de indicarse, no será posible que dichos accesos puedan realizarse indiscriminadamente por "cualquier persona que tenga acceso al programa", como se señala en la consulta, no perdiéndose además por el Centro el control sobre la información, dado que esta permanecería en sus ficheros y podría ser únicamente comunicada a otros usuarios autorizados en caso de que exista legitimación suficiente para ello.
De las normas reguladoras de los ficheros no se desprende, sin embargo la existencia de un acceso indiscriminado por cualquier usuario a los datos del sistema, estableciéndose únicamente como origen de la información los "centros educativos dependientes de la consejería de educación" y no previéndose cesiones de los datos a terceros, por lo que no es posible conocer si efectivamente el sistema permite ese acceso indiscriminado o si, por el contrario, los accesos a los datos se vincularán al hecho de que el alumno lo es del centro que accede o a que los accesos por la Administración se encuentren amparados por la Ley, estableciéndose así distintos perfiles de usuario autorizado que comportarían la licitud de las cesiones efectuadas.
En este sentido, debe reiterarse que la Ley Orgánica 2/2006 sí autoriza la cesión de datos a las Administraciones Educativas en cuanto sean necesarios para el sistema educativo, lo que habilitará la comunicación por los Centros concertados a la Administración competente de los datos necesarios para el adecuado ejercicio por ésta de las competencias que la Ley le atribuye.
De este modo, los datos relacionados con la escolarización del alumno, la solicitud de plaza en un determinado centro, el otorgamiento de ayudas y usos de servicios complementarios en los centros, públicos o concertados, e incluso los datos relacionados con la condición de usuario del sistema del propio alumno o de sus padres o tutores sí podrán ser objeto de cesión a la Administración autonómica, al encontrarse vinculadas al ejercicio de las competencias atribuidas a la misma por la legislación estatal o autonómica en la materia.
En cuanto a los datos referidos a la incapacidad de los alumnos, debe tenerse en cuenta que el artículo 75.1 de la Ley Orgánica 2/2006 dispone que "con la finalidad de facilitar la integración social y laboral del alumnado con necesidades educativas especiales que no pueda conseguir los objetivos de la educación obligatoria, las Administraciones públicas fomentarán ofertas formativas adaptadas a sus necesidades específicas". En particular, según el artículo 75.2, "las Administraciones educativas establecerán una reserva de plazas en las enseñanzas de formación profesional para el alumnado con discapacidad".
Igualmente, en el marco de la Ley 17/2007, dispone el artículo 113.1 que "el Sistema Educativo Público de Andalucía garantizará el acceso y la permanencia en el sistema educativo del alumnado con necesidad específica de apoyo educativo", definiendo el apartado 2 como alumnado con necesidades específicas de apoyo educativo, entre otros, a "aquel que presenta necesidades educativas especiales debidas a diferentes

grados y tipos de capacidades personales de orden físico, psíquico, cognitivo o sensorial".
En relación con este alumnado, dispone el artículo 113.6 de la Ley 12/2007 que "la escolarización del alumnado con necesidades específicas de apoyo educativo garantizará las condiciones más favorables para el mismo. La Administración educativa realizará una distribución equilibrada de este alumnado entre los centros docentes sostenidos con fondos públicos, en condiciones que faciliten su adecuada atención educativa y su inclusión social. A tales efectos, se podrá reservar hasta el final del período de matrícula una parte de las plazas de los centros públicos y privados concertados".
El cumplimiento de los deberes impuesto a la Administración educativa por el precepto que acaba de referirse sólo podrá llevarse a cabo conociendo las circunstancias de los alumnos con necesidades especiales que se encuentren escolarizados, dado que en caso contrario la Administración autonómica carecería de medios para garantizar la adecuada distribución equilibrada del alumnado.
En consecuencia, la comunicación a la Administración de los datos referidos a alumnos con necesidades específicas y de los datos de salud adecuados a los mismos se encontrará amparada por el artículo 113.6 de la Ley 17/2007, en conexión con la disposición adicional vigésimo tercera, apartado 4, de la Ley Orgánica 2/2006 y con el artículo 11.2 a) de la Ley Orgánica 15/1999.
Por último, en relación con las sanciones impuestas por el centro concertado por vulneración de los deberes de convivencia, la legislación con rango de Ley, estatal o autonómica no habilita una comunicación indiscriminada de los datos a la Administración. En este sentido se pronunció la Agencia Española de Protección de Datos al emitir informe en relación con la norma de creación de los ficheros gestionados en el ámbito de los programas SÉNECA y PASEN, emitido en fecha 4 de abril de 2006, en que se instaba a la Junta de Andalucía a la inclusión en el fichero de "seguimiento de conductas contrarias a la convivencia y absentismo del alumnado" a que se indicase la norma habilitante del tratamiento, habiendo sido incluida en la Orden de 20 de julio de 2006 una referencia exclusiva a normas de rango reglamentario, lo que no resulta suficiente para amparar la cesión a la Consejería en el artículo 11.2 a) de la Ley Orgánica 15/1999.
No obstante, debe tenerse en cuenta que la Ley Orgánica 2/2006 sí establece una regla general de comunicación de los datos a la Administración Educativa para el ejercicio de sus competencias, entre las que se encuentra la de inspección de los centros educativos, con las funciones expresamente atribuidas a la misma por el artículo 151 de la propia Ley Orgánica 2/2006.
El artículo 153 de dicha Ley Orgánica establece que:
"Para cumplir las funciones de la inspección educativa los inspectores tendrán las siguientes atribuciones:
a) Conocer directamente todas las actividades que se realicen en los centros, a los cuales tendrán libre acceso.
b) Examinar y comprobar la documentación académica, pedagógica y administrativa de los centros.
c) Recibir de los restantes funcionarios y responsables de los centros y servicios educativos, públicos y privados, la necesaria colaboración para el desarrollo de sus actividades, para cuyo ejercicio los inspectores tendrán la consideración de autoridad pública.
d) Cualesquiera otras que le sean atribuidas por las Administraciones educativas, dentro del ámbito de sus competencias."
En el ámbito de Andalucía, el artículo 145.2 de la Ley 17/2007 dispone que "las funciones de la inspección educativa y las atribuciones de los inspectores e inspectoras de educación son las recogidas, respectivamente, en los artículos 151 y

153 de la Ley Orgánica 2/2006, de 3 de mayo. Asimismo, los inspectores e inspectoras de educación tendrán atribuciones para requerir a los directores, directoras y titulares de los centros docentes, así como a los responsables de los distintos servicios y programas, para que adapten sus actuaciones a la normativa vigente, y para mediar en los conflictos que pudieran producirse entre los distintos miembros de la comunidad educativa, de acuerdo con lo que a tales efectos se determine".

Añade el artículo 148 que "en el desempeño de sus funciones, los inspectores e inspectoras de educación tendrán la consideración de autoridad pública, y, como tales, recibirán de los distintos miembros de la comunidad educativa, así como de las demás autoridades y funcionarios, la ayuda y colaboración precisas para el desarrollo de su actividad".

Si bien el artículo 149 de la Ley considera la visita de inspección como instrumento básico de la función inspectora, no debe olvidarse que como acaba de quedar dicho la inspección podrá, conforme al artículo 153 de la Ley Orgánica 2/2006 acceder a la documentación del centro para el adecuado cometido de sus funciones, por lo que la cesión de los datos con fines de inspección sí se encontrará habilitada por la Ley Orgánica 15/1999.

En todo caso, la habilitación que acaba de indicarse no podrá considerarse genérica, sino que debería ir referida a actuaciones concretas de inspección, a fin de que el tratamiento pueda considerarse amparado por los principios de calidad de datos consagrados por el artículo 4 de la Ley Orgánica 15/1999.

De este modo, si los sistemas SÉNECA y PASEN se encuentran configurados y gestionados de modo que los accesos por parte de los usuarios, a través de la atribución de distintos perfiles, se limitan a los señalados a lo largo de este informe, su existencia no resultará contraria a lo dispuesto en la Ley Orgánica 15/1999.

VII

De lo señalado hasta el presente lugar cabe extraer las siguientes conclusiones:

PRIMERA.- Teniendo en cuenta lo dispuesto en la Orden de 20 de julio de 2006, los sistemas SÉNECA y PASEN se configuran como aplicaciones cuyo uso deberá llevarse a cabo en el marco del Sistema Educativo Público Andaluz.

SEGUNDA.- En consecuencia, deberá diferenciarse la propia herramienta de gestión de los ficheros creados como consecuencia de su utilización por los centros. En este caso, el tratamiento o cesión de datos deberán ser conformes a lo dispuesto en los artículos 6, 7 y 11 de la Ley Orgánica 15/1999.

TERCERA.- La disposición adicional vigésimo tercera de la Ley Orgánica 2/2006 establece los criterios legitimadores de los tratamientos y cesiones de datos en el ámbito educativo, habilitando en su apartado 1 el tratamiento de los datos por los propios centros, en su apartado 2 la cesión de datos a otros centros en caso de que el alumno cambiase de centro y en su apartado 4 la cesión de datos a la administración educativa.

CUARTA.- Respecto de las cesiones a las que se refiere expresamente la consulta, la transmisión a través del sistema de los datos relacionados con los alumnos con necesidades especiales se encontrará habilitada por el artículo 11.2 a) de la Ley Orgánica 15/1999. Esta misma norma habililtará la comunicación de datos relacionados con conductas contrarias a la convivencia a la inspección educativa cuando así se requiriera en el marco de un expediente concreto. En los demás supuestos la legislación educativa estatal o autonómica no habilita la comunicación de datos de esta naturaleza a la Administración.

QUINTA.- En consecuencia, si el sistema se encuentra configurado de forma tal que los accesos a los datos, a través de distintos perfiles de usuario y la adopción de las correspondientes medidas de seguridad, se limiten a los que han sido descritos en el presente informe, no existirá vulneración de la Ley Orgánica 15/1999 como consecuencia del tratamiento de los datos a los que se refiere la consulta.

Informe Jurídico 0110-2008: sobre el tratamiento de datos por los centros de enseñanza

La consulta plantea diversas cuestiones relacionadas con la aplicación de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, en el ámbito de actividad de la consultante.

I

La primera de las cuestiones se refiere a la aplicación de la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo de educación, haciéndose referencia a su apartado 2.

La citada disposición adicional establece, con carácter general, en su apartado 1 que "los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos".

Añade el apartado 2 al que se refiere la consulta que "los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso".

De lo previsto en ambos apartados se desprende la existencia de una habilitación legal para el tratamiento por los centros educativos de los datos de los alumnos y de los relacionados con su entorno familiar y social que sean necesarios para el adecuado cumplimiento de la función educativa, descrita por el apartado 2 en sus vertientes docente y orientadora.

El artículo 6.1 de la Ley Orgánica 15/1999 establece como principio general que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa". En relación con los daos relacionados con la salud de los afectados, aclara el artículo 7.3 que "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

Pues bien, como se ha indicado, la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006 establece una habilitación legal para el tratamiento de los datos que excluye la necesidad de que el afectado o su representante legal otorgue el consentimiento para el tratamiento de cuantos datos sean necesarios para el desempeño de las funciones docente y orientadora, siempre que el tratamiento resulte efectivamente necesario para el ejercicio de tales funciones.

De este modo, dado que no será preciso el consentimiento ni del alumno ni de sus padres o tutores para el tratamiento de los datos, no podrán éstos manifestar su negativa al tratamiento. Por el contrario la propia Ley impone a los padres y alumnos un deber de cooperación en la obtención y tratamiento de los datos que podrá ser directamente invocado por el Centro en caso de existir resistencia a facilitar las citadas informaciones.

En todo caso, debe reiterarse que la propia Ley Orgánica limita el alcance de los datos que habrán de ser objeto de tratamiento a los que resulten estrictamente necesarios para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.

Con ello, se reflejan en el ámbito educativo los principios consagrados por los apartados 1 y 2 del artículo 4 de la Ley Orgánica 15/1999. Según el primero de ellos "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".
A tenor del segundo de los preceptos citados "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".

II

En segundo lugar, la consulta se refiere a la conformidad con lo dispuesto en la Ley Orgánica 15/1999 del artículo 3 de la Orden Foral 42/2000, de 18 de febrero, reguladora de aspectos relativos a la prueba de acceso a la Universidad en la Comunidad Foral de Navarra
Según indica su exposición de motivos, el objeto de la citada Orden Foral "es la regulación de la prueba de acceso que, por razón de la propia estructura de Bachillerato y de la lengua cooficial, afecta en la Comunidad Foral de Navarra, a la configuración de la comisión organizadora de la prueba de acceso y a la estructura y realización de los ejercicios de que consta la misma. Así, dispone el artículo 1 que "la presente Orden Foral será de aplicación a la Universidad Pública de Navarra, a los Centros e Institutos de Educación Secundaria con sede en el ámbito territorial de la Comunidad Foral de Navarra y a los alumnos que cursan las enseñanzas de Bachillerato en esta Comunidad", añadiendo el artículo 2 que "los alumnos realizarán la inscripción y la prueba de acceso a estudios universitarios en la Universidad Pública de Navarra. Corresponde a esta Universidad la coordinación, gestión y tramitación de la información de los Centros necesaria para la preparación de las pruebas de acceso".
El artículo 3, al que se refiere la consulta, completa los preceptos precedentes, disponiendo que "los Centros e Institutos de Educación Secundaria remitirán a la Universidad Pública de Navarra durante el mes de febrero los datos de los alumnos matriculados en segundo curso de Bachillerato. Con posterioridad, y en los plazos que determine la Universidad, presentarán una relación certificada de esos alumnos, ordenada en función de la vía por la que concurren, indicando la nota media de Bachillerato que consta en la documentación oficial y la materia de modalidad seleccionada. Toda la información será remitida en soporte informático".
Se prevé así en la Orden una cesión de datos a la Universidad Pública de Navarra, fundada en la competencia de la misma en "la coordinación, gestión y tramitación de la información de los Centros necesaria para la preparación de las pruebas de acceso". De ello se desprende que la cesión se efectúa en cuanto resulta necesaria para el desarrollo de las pruebas de acceso.
En consecuencia, la comunicación de los datos de los alumnos que cursen el segundo alo del Bachillerato puede considerarse fundada en lo dispuesto en el artículo 11.2 c) de la Ley Orgánica 15/1999, según el cual será posible la cesión sin contar con el consentimiento del afectado "Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros".
En este supuesto, la cesión se fundaría en la necesidad de que la Universidad Pública de Navarra, a la que corresponden las competencias en relación con la coordinación, gestión y tramitación de las pruebas pueda adoptar las medidas necesarias para garantizar su adecuada celebración.
La consulta señala que del tenor del artículo 3 de la Orden Foro se desprende la comunicación a la Universidad de los datos de todos los alumnos, con independencia de si los mismos van a participar o no en las pruebas de acceso.

Sin embargo, no debe olvidarse que el precepto prevé dos comunicaciones de datos: una primera cesión durante el mes de febrero, referida únicamente a “los datos de los alumnos matriculados en segundo curso de Bachillerato” y una posterior cesión, más próxima a la celebración de las pruebas, que consistirá en “una relación certificada de esos alumnos, ordenada en función de la vía por la que concurren, indicando la nota media de Bachillerato que consta en la documentación oficial y la materia de modalidad seleccionada”.

Del tenor del precepto se desprende que la primera remisión tiene por objeto la preparación y organización de las pruebas de acceso, que se concretará definitivamente en la segunda remisión, en la que sí se harán constar únicamente los datos de los alumnos que efectivamente tomarán parte en las pruebas, a tenor de la información que habrá de ser comunicada. No obstante, la información contenida en la primera remisión sí será necesaria para facilitar la mencionada organización.

Por otra parte, la información remitida en el primer momento incluiría los datos de todos los posibles participantes en las pruebas de acceso, dado que no es inequívocamente posible determinar en ese momento si un determinado alumno tomará o no finalmente parte en las pruebas, por lo que la remisión parcial de la información podría resultar inadecuada para la correcta preparación de las pruebas.

En todo caso, será preciso volver a traer a colación lo dispuesto en el artículo 4.1 de la Ley Orgánica 15/1999 y que. Aplicado al supuesto ahora analizado, implicará que los datos enviados en la primera remisión únicamente será tratados por la Universidad dentro de sus funciones de coordinación, gestión y tramitación de la información de los Centros necesaria para la preparación de las pruebas de acceso, por lo que si los datos del alumno finalmente no aparecen en la segunda remisión de información la Universidad no podrá hacer otro uso de la información.

III

La consulta se refiere, por otra parte, a la posición del centro consultante en relación con su participación en la tramitación de ayudas concedidas por las Administraciones Públicas a los alumnos del centro.

Según se indica, cabe diferenciar dos supuestos: aquéllos en los que la posición del centro es la de mero tramitador de las solicitudes dirigidas a las Administraciones públicas y aquéllos otros en los que el centro ha de tratar los datos de los beneficiarios de las ayudas “para controlar el pago de las ayudas que deben realizarse a través del Colegio”, dado que “hay ayudas que se ingresan en la cuenta del Colegio y éste las entrega a las familias”.

El segundo de los supuestos planteados presenta, a nuestro juicio, menores dudas desde el punto de vista de la aplicación de la Ley Orgánica 15/1999, debiendo considerarse que el centro tendrá en relación con el tratamiento de los datos de gestión de las ayudas la condición de responsable del tratamiento, al corresponder a su esfera la capacidad de decisión sobre la finalidad, contenido y uso del tratamiento.

En este sentido, se señala en la consulta que el consultante no ha decidido recoger los datos, por lo que no cabría considerar al mismo responsable del fichero. Sin embargo, el hecho de que los datos de los solicitantes y beneficiarios de las ayudas se recojan a instancia de los propios solicitantes o como consecuencia de la decisión de otorgarse dichas ayudas a los beneficiarios no altera la consideración de responsable del centro consultante, dado que el tratamiento se llevará a cabo en el marco de la actuación del centro y del régimen establecido por la normativa estatal y autonómica aplicable en materia de educación, produciéndose un ingreso en la cuenta del Colegio que el mismo habrá de destinar a la finalidad correspondiente en el marco de su propia actividad.

En este sentido, es claro que el centro no resolverá por sí mismo la solicitud de una determinada ayuda, en los términos que prevea la normativa aplicable. Sin embargo, una vez concedida dicha ayuda se producirá, en caso de seguirse el esquema al que

nos venimos refiriendo, un ingreso en la cuenta del centro que se corresponderá con el importe en que el beneficiario verá reducida su obligación como consecuencia de la ayuda concedida, por lo que los datos serán tratados como parte de la cuantía que el beneficiario habría de satisfacer al centro.
Del mismo modo, en caso de que la ayuda hubiera de ser finalmente facilitada al beneficiario, el centro es el receptor originario de aquélla, debiendo darle, dentro de su propia actividad, el destino legalmente exigido.
En ambos casos cabe concluir que la actuación llevada a cabo por el centro una vez percibida la ayuda es realizada en nombre propio y no como una simple prestación de servicios a la Administración educativa, lo que conduce a considerar que el centro tendrá la condición de responsable del fichero.
Del mismo modo, en el supuesto en que la actuación del centro sea la de mero tramitador de las solicitudes, el tratamiento de los datos realizado para la conservación de la acreditación de las solicitudes efectuadas debería ser considerado como propio de un responsable del fichero, con independencia de que no haya sido el centro, sino los propios solicitantes, quien haya decidido solicitar la ayuda, debiendo darse cumplimiento a lo dispuesto en la Ley Orgánica 15/1999.
En todo caso, las comunicaciones de datos del centro a la Administración concedente y de esta al centro se encontrarán amparadas por lo dispuesto en el artículo 11.2 c) de la Ley Orgánica 15/1999, al que ya se ha hecho referencia.

IV

En lo que atañe a la conservación de los datos contenidos en los ficheros de la consultante, debe tenerse en cuenta como principio esencial lo dispuesto en el artículo 4.5 de la Ley Orgánica 15/1999, que dispone que “Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados”. De este modo, los datos “no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados”.
El precepto, como señala la consulta, debe ponerse en relación con las normas previstas en el artículo 16 de la Ley Orgánica en relación con el ejercicio por el afectado del derecho de cancelación.
En particular, el artículo 16.5 dispone que “los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”.
Además, el artículo 16.3 especifica el efecto de la cancelación, que no será el borrado físico de los datos, sino que se establece que “la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión”.
La pluralidad de ficheros de los que puede resultar responsable la consultante impide determinar terminantemente que los datos únicamente hayan de ser conservados durante los plazos de prescripción establecidos en la normativa de protección de datos, debiendo los mismos permanecer en los ficheros de la consultante en cuanto puedan ser necesarios para el ejercicio de alguna acción por parte del propio alumno afectado.
Así sucederá, por ejemplo, en relación con el expediente académico, en que es posible que los datos puedan ser solicitados a instancia del propio alumno con posterioridad al transcurso de los plazos de prescripción de las infracciones en materia de protección de datos.
En este sentido, no corresponde a esta Agencia determinar el plazo de conservación de los datos del expediente académico, debiendo ser las Administraciones

competentes en la materia quienes fijen esos plazos de forma acorde con lo dispuesto en la normativa educativa y la Ley Orgánica 15/1999. Así se indicaba en las recomendaciones emitidas por esta Agencia, en relación tanto con los centros públicos, como con los privados y los concertados que "no se conoce hasta qué punto es necesario conservar toda la documentación, de cualquier naturaleza, relativa a un alumno en su expediente académico. Por ello, resultaría preciso definir hasta dónde alcanzan las responsabilidades de los centros escolares en relación con el contenido y custodia de los expedientes académicos".

En otros supuestos, como en lo que se refiera a las ayudas percibidas o en caso de centros concertados las cantidades recibidas de la Administración Educativa es posible que los plazos excedan igualmente del establecido en la Ley Orgánica 15/1999, debiendo, por ejemplo, tenerse en cuenta lo establecido en la legislación presupuestaria estatal o autonómica.

Además, junto con los ficheros de los que sea responsable el centro educativo en relación con la función estrictamente docente, el centro será igualmente responsable de otros ficheros en que los datos será tratados con otros fines, como los que contendrán los datos del personal docente o administrativo, en que será necesario atender a otras disposiciones para determinar el plazo de conservación de los datos.

En consecuencia, no resulta posible dar una respuesta única a la cuestión planteada, debiendo estarse a la naturaleza de cada tratamiento llevado a cabo y a las normas aplicables al mismo para poder establecer una respuesta a cada situación concreta.

V

Por último, se plantean determinadas cuestiones relacionadas con la inclusión de datos de salud en los partes de baja de los trabajadores y las medidas de seguridad que deberán implantarse sobre los ficheros en que consten estos datos.

Como regla general, debe recordarse que el artículo 81.6 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real decreto 1720/2007, de 21 de diciembre, establece que "podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos".

En relación con la aplicación de este precepto a los ficheros de los empleados, la cuestión ha sido analizada detalladamente en informe de esta Agencia de 1 de julio de 2008, en cuyas conclusiones se señalaba que "serán únicamente exigibles las medidas de seguridad de nivel básico en aquellos ficheros que contengan exclusivamente uno o varios de los siguientes datos:

- La indicación del grado o porcentaje de minusvalía del afectado o de los miembros de su unidad familiar a los efectos previstos para el cálculo de las retenciones en la legislación reguladora del Impuesto sobre la Renta de las Personas Físicas.
- La indicación del datos "apto" o "no apto" de un trabajador a los efectos previstos en la Ley de Prevención de Riesgos Laborales.
- Los datos relacionados con las obligaciones impuestas al empresario por la legislación vigente en materia de seguridad social que se limiten a señalar únicamente la existencia o no de enfermedad común, enfermedad profesional o accidente laboral o no laboral, así como la incapacidad laboral del trabajador.

Por el contrario, si el fichero contuviera cualesquiera datos relacionados con los resultados de las acciones de vigilancia de la salud distintos del meramente referido a la aptitud del trabajador o incorporasen los datos relacionados con la concreta enfermedad o accidente padecido por el trabajador no será posible entender aplicable el artículo 81.6 del Reglamento, debiendo implantarse las medidas de seguridad de nivel alto".

Por otra parte, los partes de baja por incapacidad facilitados al empresario no contendrán, según establece la normativa aplicable a la materia los datos concretos referidos a la enfermedad que ha justificado esa incapacidad, sino únicamente la concreta situación que motiva la baja; es decir, la concurrencia de enfermedad común o profesional o accidente laboral, siendo así de aplicación las conclusiones a las que se acaba de hacer referencia.

En el supuesto en que los justificantes en soporte papel contuvieran dichos datos, frente a lo que acaba de indicarse, las medidas a implantar en relación con el fichero no automatizado que contuviera tales datos sería, conforme a las conclusiones señaladas, las de nivel alto.

No obstante, debe recordarse que el artículo 81.8 del Reglamento dispone que “a los efectos de facilitar el cumplimiento de lo dispuesto en este Título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad”.

En consecuencia, sería posible establecer una disgregación en el fichero, de forma que las medidas de seguridad de nivel alto únicamente podrían implantarse en relación con la parte no automatizada del fichero y, en particular, en relación con los partes en soporte papel en que constasen los datos concretos relacionados con la enfermedad que justificó la situación de incapacidad del trabajador.

Informe jurídico 124/2008 sobre: La comunicación del Padrón a los colegios públicos para la escolarización de los alumnos

La consulta plantea si resultaría conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la obtención de datos del Padrón Municipal de Habitantes por un centro público de enseñanza para realizar un envío de información referida al mismo a los hogares en que residan niños en edad de escolarización.

La comunicación de datos solicitada constituye, conforme a lo dispuesto en el artículo 3 i) de la citada Ley Orgánica, una cesión de datos de carácter personal, definida como "Toda revelación de datos efectuada a persona distinta del interesado".

Tal y como determina el artículo 11.1 de la Ley Orgánica 15/1999, "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Esta regla de consentimiento sólo se verá exceptuada en los supuestos contemplados en el artículo 11.2, entre los que cabe destacar aquellos casos en que una norma con rango de Ley dé cobertura a la cesión. Por ello, deberá determinarse si la legislación reguladora de los ficheros a los que la consulta se refiere permite esa transmisión de sus datos.

Por otro lado, siendo el Padrón un fichero de titularidad pública, debe partirse, del principio de delimitación de la finalidad en las cesiones entre Administraciones Publicas consagrado por el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, al exigir que si los datos son cedidos a otras Administraciones Publicas sirvan sólo para el ejercicio de competencias iguales o que versen sobre materias semejantes, con la única excepción, tras la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, de que el cambio de finalidad esté fundado en una de las causas contenidas en el artículo 11 de la propia Ley Orgánica, pudiendo ser sustituida la necesidad del consentimiento para el cambio de finalidad por una previsión realizada en una disposición con rango de Ley (art.11.2 a).

En cuanto al Padrón municipal, el artículo 16.3 de la Ley reguladora de las bases del régimen local, redactado conforme a lo establecido en la Ley Orgánica 14/2003, de 20 de noviembre, dispone que "los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública".

Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

A la vista de lo dispuesto en el precepto transcrito y el artículo 27.5 de la Constitución Española que dispone "Los poderes públicos garantizarán el derecho de todos a la educación mediante un programación general de la enseñanza con participación efectiva de todos los afectados y la creación de centros docentes", podemos concluir que la comunicación de los datos a los que se refiere la consulta dado que se efectuará a un colegio público, que depende de la consejería de educación del Ayuntamiento consultante y siendo el domicilio un requisito fundamental a la hora de escolarizar a los niños, dicha comunicación podrá considerarse amparada en lo dispuesto en el artículo 11.2 a) de la Ley Orgánica 15/1999".

Informe jurídico 0152/2008 sobre: La publicación desglosada de la lista de admitidos en colegios públicos y privados concertados

La consulta plantea si resulta conforme con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la publicación de las listas de admitidos en los colegios públicos y privados concertados, de manera desglosada.
La fijación de criterios desglosado, y su posterior publicación en los tablones de anuncios, la misma supone una cesión de datos de carácter personal, definida en el artículo 3 i) de la Ley Orgánica 15/1999, como "Toda revelación de datos realizada a una persona distinta del interesado". Y permitirá que se comuniquen a terceros datos especialmente protegidos, tales como los relativos a la minusvalía, pues si en el criterio 1.4 relativo a la discapacidad un Solicitante tiene x puntos, esto se debe, a que en él o en alguno de sus hijos concurre alguna causa de discapacidad.
Siendo el dato de minusvalía un dato relativo a la salud de las personas resulta de aplicación el artículo 7.3 de la Ley Orgánica que dispone "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga la Ley o el afectado consienta expresamente"
En consecuencia, la publicación de los criterios desglosados, lleva implícita la comunicación a terceros de datos especialmente protegidos, por tanto, para que dicha publicación sea ajustada a la Ley Orgánica, deberá de haberse obtenido previamente el consentimiento expreso de cada uno de los afectados.
Asimismo el Decreto 6/2007, de 26 de marzo, por el que se regula la admisión del alumnados de enseñanzas no universitarias en los centros docentes públicos y privados concertados que viene a desarrollar y aplicar en la Comunidad Autónoma de Canarias la Ley Orgánica 2/2006, de 3 de mayo de educación, determina en su artículo14 que "Los centros docentes publicarán en el tablón de anuncios, en el plazo que se determine, la relación de alumnos admitidos y no admitidos, con especificación de la puntuación obtenida una vez aplicados los criterios previstos en los artículos 9 y 10 del presente Decreto"
El artículo anteriormente trascrito no habilita la publicación desglosada de la puntuación obtenida por cada criterio, sino que determina que se publicará la puntuación total, después de aplicar los criterios fijados en los artículos 9 y 10 del mencionado Decreto. Asimismo dicho Decreto, no sería suficiente, desde el prisma de la jerarquía normativa, dado que no tiene valor de Ley, para acordar la publicación de datos especialmente protegidos.
Por último, a efectos informativos indicar que la Agencia Española de Protección de Datos, en el informe de 6 de septiembre de 2007, analiza la posibilidad de hacer constar, no los criterios desglosados, sino las causas de exclusión en las listas de no admitidos señalando al efecto que :
"No obstante, la comunicación de datos planteada, contenida en la notificación de la resolución del procedimiento de admitidos, deberá considerarse como cesión de datos de carácter personal, toda vez que el artículo 3 i) de la Ley Orgánica define aquélla como "toda revelación de datos realizada a una persona distinta del interesado". Si lo que pretenden es la publicación de las mencionadas listas en tablones de anuncios de las dependencias del Ayuntamiento, la misma supone una cesión de datos de carácter personal, definida en el artículo 3 i) de la Ley Orgánica 15/1999, como "Toda revelación de datos realizada a una persona distinta del interesado".
En relación con la cesión de datos, el artículo 11.1 de la Ley dispone que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Este consentimiento sólo se verá exceptuado en los supuestos contemplados en el artículo

11.2, cuyo apartado a) prevé la posible cesión inconsentida de los datos cuando una norma con rango de Ley así lo disponga.
En el supuesto que se plantea, si las bases de la convocatoria para la admisión en la escuela infantil, prevén la publicación de las listas de admitidos y excluidos, incluidas las causas de la exclusión, los participantes en las mismas habrán dado su consentimiento previo a la citada cesión de sus datos cuando aceptaron las bases y efectuaron su solicitud de participación en las mismas. En ese caso, podría entenderse implícitamente prestado el consentimiento con la aceptación de las bases de la convocatoria y sería correcta la publicación de los referidos datos tal y como haya quedado reflejado en la misma convocatoria.
No obstante, lo dispuesto anteriormente debe ponerse en conexión con la obligación de notificar a los interesados las resoluciones administrativas que afecten a sus derechos e intereses, que establece el artículo 58 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
En dicho precepto y en el artículo siguiente (artículo 59) se regulan taxativamente los supuestos en que tal notificación se producirá de forma distinta a la notificación personal, bien mediante la publicación de las resoluciones, bien mediante su publicación en el tablón de edictos o de anuncios. Por tanto, procede analizar si, de acuerdo con la Ley Orgánica 15/1999, la previsión contenida en el artículo 59.5 de la Ley 30/1992, de 26 de noviembre, puede considerarse norma habilitadora de la cesión, mediante publicación, de los datos personales a que se refiere la Coorporación consultante en su escrito.
De acuerdo con el mencionado precepto, referido a la “Práctica de la notificación”:
“Artículo 59. Práctica de la notificación.
(...)
6. La publicación, en los términos del artículo siguiente, sustituirá a la notificación surtiendo sus mismos efectos en los siguientes casos:
a) Cuando el acto tenga por destinatario a una pluralidad indeterminada de personas o cuando la Administración estime que la notificación efectuada a un solo interesado es insuficiente para garantizar la notificación a todos, siendo, en este último caso, adicional a la notificación efectuada.
b) Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el tablón de anuncios o medios de comunicación donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos”.
Sin embargo, la propia Ley 30/1992, de 26 de noviembre, en su artículo 61, relativo a la “Indicación de notificaciones y publicaciones”, dispone que: “Si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el diario oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto y constancia de tal conocimiento”.
En conclusión, la publicación de las causas de exclusión será adecuada a la Ley Orgánica 15/1999, sí en las bases de la convocatoria se hubiese establecido como se haría pública los admitidos y excluidos, haciendo referencia a las causas de exclusión.
No obstante, sí el órgano consultante considera que la publicación de las causas de exclusión lesiona derechos e intereses legítimos podrá optar por aplicar lo dispuesto en el artículo 61 de la Ley 30/1992, antes trascrito”

Informe 0292/2008 sobre: El acceso a los expedientes por los interesados en los colegios concertados.

La consulta plantea, si los centros privados concertados vulneran, la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, sí en un procedimiento de concurrencia competitiva muestran el expediente administrativo a los interesados en dicho procedimiento.
Esta cuestión ya ha sido analizada por la Agencia Española de Protección de Datos en el informe de fecha 20 de abril de 2007, en el que se establecía que;
"Con carácter general, debe indicarse que la comunicación de datos a los que se refiere la consulta constituye, conforme a lo dispuesto en el artículo 3 i) de la Ley Orgánica 15/1999, una cesión de datos de carácter personal, definida como "Toda revelación de datos efectuada a persona distinta del interesado".
Por otra parte, la cesión o comunicación de datos de carácter personal viene regulada en el artículo 11.1 de la Ley Orgánica al establecer que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."
No obstante, el artículo 11.2 dispone que "El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando la cesión está autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica."
Teniendo en cuenta lo que se acaba de indicar, la comunicación del expediente, requerirá el consentimiento del interesado a menos que la misma pueda ampararse en alguno de los supuestos excepcionados por el citado artículo 11.2. Pudiendo resolverse la cuestión, desde el ejercicio del derecho de acceso a la documentación obrante en el procedimiento, de aquellos que tengan la consideración de interesado, por aplicación de los principios establecidos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas.
Lo que en primer lugar, nos obliga a analizar si a los centros privados concertados le resulta de aplicación la Ley 30/1992, para lo cual es necesario acudir a la regulación que existe sobre la materia.
En primer lugar Ley Orgánica 2/2006, de 3 mayo de Enseñanza en General, remite a la normativa autonómica en cuanto a la tramitación de los procedimientos, pues no son de competencia exclusiva del Estado así se deduce de lo dispuesto en su Disposición final sexta que señala "Las normas de esta Ley podrán ser desarrolladas por las Comunidades Autónomas, a excepción de las relativas a aquellas materias cuya regulación se encomienda por la misma al Gobierno o que corresponden al Estado

conforme a lo establecido en la disposición adicional primera, número 2, de la Ley Orgánica 8/1985, de 3 de julio, Reguladora del Derecho a la Educación."
La Legislación andaluza sobre la materia se concreta en el Decreto 53/2007, de 20 febrero, de la Consejería de Educación de Andalucía que regula la enseñanza no universitaria, y resulta aplicable al supuesto planteado el artículo 34. 2 que determina lo siguiente "Los acuerdos y decisiones que sobre la admisión del alumnado adopten los titulares de los centros docentes privados concertados podrán ser objeto de reclamación en el plazo de un mes ante la persona titular de la correspondiente Delegación Provincial de la Consejería competente en materia de educación, cuya resolución pondrá fin a la vía administrativa. Cuando dicha reclamación se presente ante el titular del centro docente privado concertado, éste deberá remitirla a la Delegación Provincial en el plazo de diez días, con su informe y con una copia completa y ordenada del expediente."
Por tanto, dado que la resolución de la reclamación ponen fin a la vía administrativa, ello implica que ha de tratarse de un acto administrativo, pues sólo ponen fin a dicha vía los actos administrativos, que en todo caso deberán de ajustarse a la Ley 30/1992. En definitiva podemos afirmar que a los colegios privados concertados les resulta de aplicación la Ley 30/1992.
En este sentido, el artículo 31 de la Ley 30/1992 delimita jurídicamente el concepto de interesado en el procedimiento administrativo, indicando a tal efecto que se considerarán como tales en el procedimiento "a) Quienes lo promuevan como titulares de derechos o intereses legítimos individuales o colectivos; b) Los que, sin haber iniciado el procedimiento, tengan derechos que puedan resultar afectados por la decisión que en el mismo se adopte; y c) Aquellos cuyos intereses legítimos, individuales o colectivos, puedan resultar afectados por la resolución y se personen en el procedimiento en tanto no haya recaído resolución definitiva".
Es decir, en virtud de los establecido en el artículo 31 que se cita, se puede entender por interesado en todo procedimiento sancionador aquel frente al que el procedimiento se dirige como presunto infractor de las normas administrativas.
A su vez, el artículo 35.a) de la misma Ley recoge el derecho de los ciudadanos a "A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos".
En consecuencia, aquella persona o personas que ostenten la condición de interesado en los términos del artículo 31 de la Ley 30/1992, tendrá derecho a conocer el estado de la tramitación del, resultando la comunicación de los referidos datos conforme a los establecido en el artículo 11,2.a) de la Ley 15/1999."

Informe Jurídico 0385/2008 sobre: El centro público docente, los tratamientos de datos sensibles de los alumnos. Habilitación legal, responsable y usuario de los datos.

La consulta solicita de esta Agencia información sobre las cuestiones a tener en cuenta para que el Centro que realiza la consulta se adecue a la normativa reguladora sobre protección de datos de carácter personal y en concreto a lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

I

En primer lugar plantea si el Centro Público "Equipo de Orientación Educativa y Psicopedagógica", en adelante E.O.E.P., tiene la consideración de centro docente, a los efectos de aplicar al mismo, lo dispuesto en la Disposición adicional vigésimo tercera de la Ley Orgánica de Educación 2/2006, de 3 de mayo. Al respecto, parece desprenderse de la propia denominación del centro "Equipo de Orientación Educativa y Psicopedagógica" la naturaleza de centro docente, que lo será en la medida que el mismo encaje en la definición que contiene el TIULO IV (Centros docentes) CAPITULO I (Principios generales), Régimen jurídico del artículo 107 de la Ley Orgánica de Educación cuyo número 1 establece "Los centros docentes que ofrezcan enseñanzas reguladas en esta Ley se regirán por lo dispuesto en la Ley Orgánica 8/1985, de 3 de julio, Reguladora del Derecho a la Educación, en la presente Ley Orgánica y en las disposiciones que la desarrollen, así como por lo establecido en las demás normas vigentes que les sean de aplicación, sin perjuicio de lo previsto en los apartados siguientes de este artículo."

También puede desprenderse de la consulta que el Centro acoge a alumnado con necesidad específica de apoyo educativo, respecto del cual señala el artículo 71 de la misma norma "2. Corresponde a las Administraciones educativas asegurar los recursos necesarios para que los alumnos y alumnas que requieran una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar, puedan alcanzar el máximo desarrollo posible de sus capacidades personales, y en todo caso, los objetivos establecidos con carácter general para todo el alumnado." Y en el artículo 72.1 dice que "Para alcanzar los fines señalados en el artículo anterior, las Administraciones educativas dispondrán del profesorado de las especialidades correspondientes y de profesionales cualificados, así como de los medios y materiales precisos para la adecuada atención al alumnado."

De lo indicado anteriormente cabe concluirse que el Centro dirigido por el consultante tendrá la consideración de docente en la medida que acoja a este tipo de alumnado y cumpla estas finalidades.

II Con carácter previo y a efectos de centrar la cuestión objeto de consulta, del contenido del escrito se deduce que el centro de educación que solicita la información se trata de un Centro Público dependiente de la Consejería de Educación del Gobierno de Cantabria. Sentados así los términos y como punto de partida, sí el centro educativo consultante es de titularidad pública deberá aprobarse la oportuna Disposición de Carácter General en la que se deberá de contener todas las previsiones del artículo 20 de la citada Ley Orgánica, además de inscribirse en el Registro General de Protección de Datos.

En este sentido, el artículo 55.1 del Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, establece que "Todo fichero de datos de carácter personal, de titularidad pública, será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de

Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente".
En cuanto a la obligación de notificar, esta corresponderá al responsable del fichero, definido por el artículo 3 d) de la Ley Orgánica 15/1999 como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".
Como primer paso, procede determinar a quién corresponde la obligación de adoptar la correspondiente disposición de carácter general y la consiguiente notificación del tratamiento al Registro General del Protección de Datos, resulta imprescindible delimitar si el consultante es un órgano incardinado en la Administración Autonómica o si el mismo posee personalidad jurídica independiente de la misma.
En el primer supuesto, el Centro no sería sino un mero usuario del fichero, cuyo responsable sería la Administración educativa autonómica, de forma que la obligación de notificación e implantación del resto de garantías y principios establecidos en la Ley 15/1999 y su normativa de desarrollo, correspondería a la Consejería de Educación, debiendo hacerse referencia al Centro educativo únicamente como lugar de ubicación del fichero. En caso contrario, el responsable del fichero sería el propio Centro, correspondiendo al mismo la notificación del tratamiento al Registro de esta Agencia.
Según dispone el artículo 108 de la Ley Orgánica 2/2006, de 3 de mayo, de educación y de enseñanza en general, "Los centros docentes se clasifican en públicos y privados", añadiendo que "Son centros públicos aquellos cuyo titular sea una administración pública".
En consecuencia, dicha Ley Orgánica vincula el carácter público de los Centros con la titularidad de los mismos. Al propio tiempo, la misma no establece en ningún lugar si los centros tendrán o no personalidad jurídica dependiente de la correspondiente Administración Educativa, si bien especifican expresamente los ámbitos en que los mismos gozarán de autonomía pedagógica, organizativa y de gestión económica (artículo 120 de la Ley Orgánica).
En el ámbito de la Comunidad Autónoma de Cantabria el Decreto 126/2004, de 18 de noviembre, regula la creación de los Centros de Educación Obligatoria, y dispone en su artículo 1 que "Son Centros de Educación Obligatoria aquellos centros docentes públicos en los que se imparta Educación Primaria y todos los cursos de Educación Secundaria Obligatoria. Se ubicarán en ámbitos rurales, escolarizándose en un mismo centro los niveles obligatorios y gratuitos. Así mismo, cuando las circunstancias así lo requieran, podrán impartir Educación Infantil y, en su caso, Preescolar.
A su vez, el artículo 2.1 señala que "La creación y supresión de los Centros de Educación Obligatoria corresponde al Gobierno de Cantabria, a propuesta de la Consejería competente en materia de educación."
De lo dispuesto en la legislación básica estatal y en la autonómica a la que acaba de hacerse referencia se desprende que los Centros Públicos de Educación Obligatoria, que incluiría al Centro E.O.E.P. de Reinosa consultante no son sino órganos directamente dependientes de la Consejería autonómica y carentes de personalidad propia y diferenciada de la misma, sin perjuicio de las peculiaridades que les son propias en lo referente al respeto de los principios de autonomía pedagógica, organizativa y de gestión económica que la Ley Orgánica de Educación 2/2006 establece.
Por ello, ha de concluirse que, integrados orgánicamente en la Administración autonómica, será ésta la obligada al cumplimiento de las obligaciones que respecto de los ficheros de titularidad pública impone la Ley Orgánica 15/1999, debiendo la misma adoptar la correspondiente disposición de carácter general y proceder a la notificación de los tratamientos al Registro General de Protección de Datos, en la que se hará constar que el Centro es el lugar de ubicación del fichero.

Por último a través de la dirección www.agpd.es , en el apartado canal del responsable es posible obtener amplia información sobre las medidas que deban adoptarse para el cumplimiento de la Ley. En especial se informa que en el apartado Canal de Documentación > Recomendaciones, se incluye el texto de las Recomendaciones adoptadas por el Director de la Agencia relativas al Plan sectorial de oficio realizado a la enseñanza reglada no Universitaria, de 29 de diciembre de 2006, al objeto de adecuar los tratamientos de datos a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

III Otra de las cuestiones se refiere a la aplicación de la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo de Educación, haciéndose referencia a su apartado 2.

La citada disposición adicional establece, con carácter general, en su apartado 1 que "los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos".

Añade el apartado 2 al que se refiere la consulta que "los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso".

De lo previsto en ambos apartados se desprende la existencia de una habilitación legal para el tratamiento por los centros educativos de los datos de los alumnos y de los relacionados con su entorno familiar y social que sean necesarios para el adecuado cumplimiento de la función educativa, descrita por el apartado 2 en sus vertientes docente y orientadora.

El artículo 6.1 de la Ley Orgánica 15/1999 establece como principio general que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa". En relación con los datos relacionados con la salud de los afectados, aclara el artículo 7.3 que "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente".

Pues bien, como se ha indicado, la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006 establece una habilitación legal para el tratamiento de los datos que excluye la necesidad de que el afectado o su representante legal otorgue el consentimiento para el tratamiento de cuantos datos sean necesarios para el desempeño de las funciones docente y orientadora, siempre que el tratamiento resulte efectivamente necesario para el ejercicio de tales funciones.

De este modo, dado que no será preciso el consentimiento ni del alumno ni de sus padres o tutores para el tratamiento de los datos, no podrán éstos manifestar su negativa al tratamiento. Por el contrario, la propia Ley impone a los padres y alumnos un deber de cooperación en la obtención y tratamiento de los datos que podrá ser directamente invocado por el Centro en caso de existir resistencia a facilitar las citadas informaciones. La conclusión anterior sirve así para dar respuesta a la consultante sobre si se necesita o no el consentimiento de los menores de 14 años para el tratamiento de los datos de los alumnos ya referidos.

Por otra parte, la Ley Orgánica 2/2006 de Educación, habilita dicha cesión también en sus artículos 71 y 72 que disponen que "1. Las Administraciones educativas dispondrán los medios necesarios para que todo el alumnado alcance el máximo desarrollo personal, intelectual, social y emocional, así como los objetivos establecidos con carácter general en la presente Ley.
2. Corresponde a las Administraciones educativas asegurar los recursos necesarios para que los alumnos y alumnas que requieran una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar, puedan alcanzar el máximo desarrollo posible de sus capacidades personales y, en todo caso, los objetivos establecidos con carácter general para todo el alumnado.
3. Las Administraciones educativas establecerán los procedimientos y recursos precisos para identificar tempranamente las necesidades educativas específicas de los alumnos y alumnas a las que se refiere el apartado anterior. La atención integral al alumnado con necesidad específica de apoyo educativo se iniciará desde el mismo momento en que dicha necesidad sea identificada y se regirá por los principios de normalización e inclusión.
4. Corresponde a las Administraciones educativas garantizar la escolarización, regular y asegurar la participación de los padres o tutores en las decisiones que afecten a la escolarización y a los procesos educativos de este alumnado. Igualmente les corresponde adoptar las medidas oportunas para que los padres de estos alumnos reciban el adecuado asesoramiento individualizado, así como la información necesaria que les ayude en la educación de sus hijos.
Artículo 72.1. Para alcanzar los fines señalados en el artículo anterior, las Administraciones educativas dispondrán del profesorado de las especialidades correspondientes y de profesionales cualificados, así como de los medios y materiales precisos para la adecuada atención a este alumnado.
2. Corresponde a las Administraciones educativas dotar a los centros de los recursos necesarios para atender adecuadamente a este alumnado. Los criterios para determinar estas dotaciones serán los mismos para los centros públicos y privados concertados.
3. Los centros contarán con la debida organización escolar y realizarán las adaptaciones y diversificaciones curriculares precisas para facilitar a todo el alumnado la consecución de los fines establecidos.
4. Las Administraciones educativas promoverán la formación del profesorado y de otros profesionales relacionada con el tratamiento del alumnado con necesidad específica de apoyo educativo.
5. Las Administraciones educativas podrán colaborar con otras Administraciones o entidades públicas o privadas sin ánimo de lucro, instituciones o asociaciones, para facilitar la escolarización y una mejor incorporación de este alumnado al centro
En todo caso, debe reiterarse que la propia Ley Orgánica limita el alcance de los datos que habrán de ser objeto de tratamiento a los que resulten estrictamente necesarios para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.
Con ello, se reflejan en el ámbito educativo los principios consagrados por los apartados 1 y 2 del artículo 4 de la Ley Orgánica 15/1999. Según el primero de ellos "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

A tenor del número 2 del artículo citado “los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos”.

IV

Analizada ya la habilitación legal que permite el tratamiento de los datos de los alumnos del centro sin necesidad de consentimiento previo, ha de señalarse que ello no excluye al responsable del mismo del deber de informar a que se refiere en su escrito, contemplado en el artículo 5.1 de la Ley Orgánica 15/1999

que dispone que “Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”. Si conforme a lo dicho más arriba de este informe, la incorporación de un alumno a un centro supone el consentimiento para el tratamiento o cesión de sus datos, sería éste el momento o trámite en el que podría reflejarse dicha información.

En relación con la cesión de listados o censos de los alumnos del centro a colegios, Consejería de Educación u otras administraciones debe señalarse que el artículo 21 de la Ley Orgánica 15/1999 dispone que “1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.(STC 292/2000, de 30 de noviembre).

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.”

Teniendo en cuenta lo señalado anteriormente, en el sentido de que la Consejería de Educación sería la responsable de los ficheros o tratamientos y que los centros pertenecientes a la misma serían usuarios de los datos y centros de ubicación de los mismos, el envío de los listados a la Consejería no sería una cesión. No obstante, la Disposición adicional vigesimotercera de la Ley Orgánica de Educación señala en su número 2 que “ La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos t, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad en los términos establecidos por ls legislación de protección de datos.” De modo que la cesión de los referidos listados a colegios queda circunscrita solo al colegio de referencia y no a otros centros en general, en aplicación de los principios que informan la protección de datos recogidos en el artículo 4.1 de la Ley Orgánica 15/1999 que exigen que la comunicación sea adecuada, pertinente y no excesiva, en relación con la finalidad para la que fueron recogidos los datos.

El artículo 71.3 de la Ley Orgánica de Educación señala que “ Las Administraciones educativas establecerán los procedimientos y recursos precisos para identificar tempranamente las necesidades educativas específicas de los alumnos y alumnas a las que se refiere el apartado anterior. La atención integral al alumnado con necesidad específica de apoyo educativo se iniciará desde el mismo momento en que dicha necesidad sea identificada y se regirá por los principios de normalización e inclusión.” De modo que la propia Ley atribuye a la Administración educativa la potestad para decidir sobre la finalidad, contenido y uso del fichero o tratamiento de datos, siendo ésta, por consiguiente la responsable del mismo, aunque no lo realice materialmente, (artículo 5 q) del Real Decreto 1720/2007, por el que se aprueba el Reglamento de

desarrollo de la Ley Orgánica 15/1999. Con lo dicho anteriormente, queda despejada la cuestión planteada por la consultante en el sentido de que la Consejería de Educación de Cantabria es la responsable del tratamiento.
Por último se plantea los términos en que se deben custodiar y realizar las actuaciones para actuar de conformidad con la Ley Orgánica 15/1999. Según se desprende de la consulta, parece que se crea un fichero de los alumnos que se hallan discapacitados, lo que implica la creación del correspondiente fichero. Por tanto sí el centro educativo consultante es de titularidad pública deberá aprobarse la oportuna Disposición de Carácter General en la que se deberá de contener todas las previsiones del artículo 20 de la citada Ley Orgánica, además de inscribirse en el Registro General de Protección de Datos.
En cuanto al tratamiento de los datos de carácter personal que se realice en el centro educativo, deberá ajustarse a lo establecido en el artículo 9 de la Ley 15/1999 según el cual, "El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite 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 del medio físico o natural."
Igualmente, al apartado tercero del mismo precepto remite a la determinación reglamentaria los requisitos y condiciones que deban reunir los ficheros y aquellas personas que intervienen en el tratamiento de datos especialmente protegidos, remisión que actualmente debe hacerse al Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, Real Decreto 1720/2007, de 21 de diciembre, cuyo TITULO VIII se refiere a las medidas de seguridad en el tratamiento de datos de carácter personal. En su atículo 88 regula el documento de seguridad y señala en su número 1 " El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información." El contenido mínimo del documento de seguridad lo recoge el número 3 de este artículo.
Por otra parte, y dado que se van a tratar datos de salud especialmente protegidos, entre otros, las medidas de seguridad a aplicar serán las de nivel alto, que exigirán, así mismo, la adopción de las medidas de nivel medio y básico contenidas en el citado Reglamento, conforme señala su artículo 81.3 a).

V

En lo que atañe a la conservación de los datos contenidos en los ficheros de la consultante, debe tenerse en cuenta como principio esencial lo dispuesto en el artículo 4.5 de la Ley Orgánica 15/1999, que dispone que "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados." De este modo, los datos "no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."
El precepto, como señala la consulta, debe ponerse en relación con las normas previstas en el artículo 16 de la Ley Orgánica en relación con el ejercicio por el afectado del derecho de cancelación.
En particular, el artículo 16.5 dispone que "los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".
Además, el artículo 16.3 especifica el efecto de la cancelación, que no será el borrado físico de los datos, sino que se establece que "la cancelación dará lugar al bloqueo de

los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión".

La pluralidad de ficheros de los que puede resultar responsable la consultante impide determinar terminantemente que los datos únicamente hayan de ser conservados durante los plazos de prescripción establecidos en la normativa de protección de datos, debiendo los mismos permanecer en los ficheros de la consultante en cuanto puedan ser necesarios para el ejercicio de alguna acción por parte del propio alumno afectado.

Así sucederá, por ejemplo, en relación con el expediente académico, en que es posible que los datos puedan ser solicitados a instancia del propio alumno con posterioridad al transcurso de los plazos de prescripción de las infracciones en materia de protección de datos.

En este sentido, no corresponde a esta Agencia determinar el plazo de conservación de los datos del expediente académico, debiendo ser las Administraciones competentes en la materia quienes fijen esos plazos de forma acorde con lo dispuesto en la normativa educativa y la Ley Orgánica 15/1999. Así se indicaba en las recomendaciones emitidas por esta Agencia, en relación tanto con los centros públicos, como con los privados y los concertados que "no se conoce hasta qué punto es necesario conservar toda la documentación, de cualquier naturaleza, relativa a un alumno en su expediente académico. Por ello, resultaría preciso definir hasta dónde alcanzan las responsabilidades de los centros escolares en relación con el contenido y custodia de los expedientes académicos".

En otros supuestos, como en lo que se refiera a las ayudas percibidas o en caso de centros concertados las cantidades recibidas de la Administración Educativa es posible que los plazos excedan igualmente del establecido en la Ley Orgánica 15/1999, debiendo, por ejemplo, tenerse en cuenta lo establecido en la legislación presupuestaria estatal o autonómica.

Además, junto con los ficheros de los que sea responsable el centro educativo en relación con la función estrictamente docente, el centro será igualmente responsable de otros ficheros en que los datos será tratados con otros fines, como los que contendrán los datos del personal docente o administrativo, en que será necesario atender a otras disposiciones para determinar el plazo de conservación de los datos.

En consecuencia, no resulta posible dar una respuesta única a la cuestión planteada, debiendo estarse a la naturaleza de cada tratamiento llevado a cabo y a las normas aplicables al mismo para poder establecer una respuesta a cada situación concreta.

VI

Por último y en relación con la información que solicita la consultante sobre las sanciones, debe tenerse en cuenta lo dispuesto por el artículo 43.2 de la Ley Orgánica 15/1999 que señala "Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2." Este artículo procede a regular las infracciones de las Administraciones Públicas diciendo "Cuando las infracciones a las que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de l Agencia de Protección de Datos dictará una resolución estableciendo las medidas para que cesen o se corrijan los efectos de la infracción. Esta resolución se comunicará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia 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 a la Agencia las resoluciones que caigan 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."
Todo ello en aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Informe 0194/2009 sobre: fotos de menores publicadas en la página web del colegio.

La consulta plantea cual es la actuación procedente, conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), ante la publicación no consentida en la página web de un centro escolar de fotos de una alumna con motivo de la realización de diversas actividades extraescolares.

La primera cuestión que resulta del presente supuesto consiste en determinar si las imágenes de la menor pueden ser consideradas como datos de carácter personal, de conformidad con lo establecido en dicha Ley.

Con carácter general, debe indicarse que los artículos 1 y 2 de la LOPD, extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento automatizado de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como "cualquier información concerniente a personas físicas identificadas o identificables".

Por su parte, el artículo 5.1 del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa que constituyen un dato de carácter personal "Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."

En consecuencia, las imágenes a las que se refiere la consulta tendrán la consideración de datos de carácter personal en caso de que las mismas permitan la identificación de las personas que en ellas aparecen, no encontrándose amparadas por la LOPD en caso contrario.

Siendo la imagen un dato personal, en los términos vistos, la toma de fotos de los alumnos efectuada por el colegio constituye, por consiguiente, un tratamiento de datos personales, tal y como prevé el artículo 3 de la LOPD que configura este como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."

En lo que se refiere al tratamiento de datos de carácter personal, entre las obligaciones del responsable del fichero, en el presente caso el centro escolar, está la de obtener el consentimiento del interesado para el tratamiento o cesión de los datos y la de informar sobre los derechos que les asisten, así como sobre la identidad y dirección del responsable y sobre el uso que se va a dar a esos datos.

En este sentido, tal y como dispone el artículo 6.1 de la LOPD, "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa". Este consentimiento deberá ser, conforme a lo dispuesto en el artículo 3 h) "libre, inequívoco, específico e informado", debiendo en consecuencia aparecer vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos, siendo así que los datos únicamente podrían ser tratados en el ámbito de las mencionadas finalidades, tal y como dispone el artículo 4.1 de la misma norma, no pudiendo ser tratados para fines incompatibles con aquéllas (artículo 4.2 de la LOPD).

La manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realiza en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información.

El deber de información al afectado aparece regulado en la LOPD por su artículo 5, cuyo apartado 1, aplicable al supuesto de recogida de datos del propio afectado, como sucedería en el caso descrito en la consulta, establece que:
"Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante."
En el presente caso, las imágenes tratadas afectan a un menor de edad, por lo que, debe tenerse en cuenta lo previsto en número primero del artículo 13 del Reglamento de desarrollo de la LOPD, según el cual "Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para suprestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores."
Asimismo, la publicación en la página web del colegio de las fotos de los alumnos constituye una cesión o comunicación de datos de carácter personal, definida por el artículo 3 j) de la LOPD como "Toda revelación de datos realizada a una persona distinta del interesado".
En relación con las cesiones de datos, prescribe el artículo 11.1 de la LOPD que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".
En consecuencia, tanto la toma de las fotografías, como su publicación en Internet requieren el consentimiento, en los términos antes señalados, del afectado o de sus padres si se trata de un menor de 14 años, de forma que cuando se tratan y ceden dichos datos personales sin el pertinente consentimiento, la LOPD establece el correspondiente mecanismo reactivo, constituido por el derecho de cancelación de datos de carácter personal, recogido en su artículo 16.
A este respecto, el artículo 31.2 del Reglamento de Desarrollo de la LOPD, precisa que "El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento".
Añade el artículo 18.2 de la LOPD que "el interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación".
Por consiguiente, los padres del menor afectado podrán ejercitar su derecho de cancelación ante el centro escolar como responsable del fichero, a fin de que se retiren las imágenes del menor de la página web. Dicho derecho deberá ser atendido en el plazo de 10 días que señala el artículo 16 de la LOPD, en otro caso, los afectados podrán recabar la tutela de esta Agencia en la forma prevista en el artículo 18 de la misma norma. Ello sin perjuicio de la posibilidad de instar de esta Agencia el ejercicio de su potestad sancionadora.
Por otra parte, cabe señalar que el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en

virtud de lo previsto en el citado artículo 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, en el Dictamen 2/2009, sobre la protección de los datos personales de los niños, en el que se contempla el especial supuesto de los colegios, recuerda, al referirse a los sitios web creados por éstos, que deben ser conscientes de que divulgar información personal justifica un cumplimiento más riguroso de los principios fundamentales de protección de datos. Igualmente recomienda que se pongan en marcha mecanismos de acceso restringido con vistas a proteger la información personal en cuestión, por ejemplo mediante la conexión con nombre de usuario y contraseña.

Asimismo, el aludido Dictamen advierte que debe prestarse una especial atención a la publicación por parte de los colegios de fotos de sus alumnos en Internet, debiendo hacerse siempre una evaluación del tipo de foto, la pertinencia de su publicación y su objetivo. Hace referencia a que incluso en aquellos casos en que se tomen fotografías colectivas que no permitan una fácil identificación de los alumnos, que podrían no estar sujetas a la normativa de protección de datos como se ha señalado al principio del presente informe, las escuelas deben informar a los niños y a sus padres de que se van a tomar fotografías y como van a utilizarse, dándoles la oportunidad de rehusar su inclusión en dicha foto.

Igualmente, debe recordarse que esta Agencia ha publicado unas recomendaciones para la protección de datos de los menores, en las que se señalaba que deben extremarse las precauciones en Internet y, en particular, se indicaba que “no es aconsejable publicar fotos que identifiquen a un niño, por ejemplo situándole en el contexto de un colegio y/o actividad determinados.”

Informe 0274/2009 sobre: cámaras video instaladas en guarderías.

La consulta solicita información para instalar una cámara de videovigilancia en una guardería pública al amparo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
En primer lugar se comunica que la Agencia Española de Protección de Datos carece de competencias para la autorización de sistemas de vidoevigilancia, siendo su competencia la de velar para que el tratamiento de datos derivado de la existencia de dichos sistemas resulte acorde a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y la Instrucción 1/2006, de 8 de noviembre de esta Agencia.
No obstante indicaremos que en la Guía de Videovigilancia publicada por la Agencia Española de Protección de Datos en el año 2009, y disponible en la página web de la Agencia www.agpd.es, dispone de la información necesaria para la instalación de cámaras, precisamente en la misma se pronuncia sobre los entornos escolares, que "*Existen servicios de valor añadido basados en la captación de imágenes. Un ejemplo cada vez más frecuente consiste en facilitar el acceso a los padres a imágenes declases y espacios de juego en guarderías o centros de educación infantil. En estecaso debe tenerse en cuenta que:*
Se aplican los principios generales de la LOPD.
El consentimiento para el tratamiento de datos de los menores se encuentra regulado en el artículo 13 RDLOPD y exige la autorización paterna, materna o del representante legal cuando se trate de menores de edad.
Debe definirse con precisión la finalidad para la captación de tales imágenes, que en todo caso respetará el principio de proporcionalidad y adecuación, y en particular los usos adicionales con fines promocionales o de marketing, memoriasescolares de actividad, o websites públicos del centro.
Deben informarse adecuadamente y respetarse los derechos de los trabajadores afectados por el uso de videocámaras como monitores, profesores, personal de limpieza etc.
Deberá garantizarse la seguridad y el secreto, en particular cuando el acceso a las imágenes se produzca online.
En aquellos casos en los que se facilite acceso a un colectivo, como el de todos los padres de un aula:
Deberán definirse los perfiles de acceso que, por ejemplo, debería limitarse a los entornos en los que se encuentren sus hijos, nunca a otras aulas.
Deberá informarse a los padres de las responsabilidades que les incumben por el acceso a los datos."
Al aplicarse los principios generales de protección de datos es preciso señalar que la grabación de las imágenes constituye un tratamiento de datos y así se establece en el artículo 2.1 de la misma señala: "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado"; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como "Cualquier información concerniente a personas físicas identificadas o identificables".
El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias". La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que

constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.
En este sentido, tal y como dispone el artículo 6.1 de la Ley Orgánica 15/1999, “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”. Este consentimiento deberá ser, conforme a lo dispuesto en el artículo 3 h) “libre, inequívoco, específico e informado”, debiendo en consecuencia aparecer vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos, siendo así que los datos únicamente podrían ser tratados en el ámbito de las mencionadas finalidades, tal y como dispone el artículo 4.1 de la Ley Orgánica, no pudiendo ser tratados para fines incompatibles con aquéllas (artículo 4.2 de la Ley Orgánica).
Respecto del tratamiento de las imágenes del profesorado, y el personal que preste servicios profesionales en el centro, deberán de otorgar su consentimiento a la captación de su imagen, lo mismo ocurrirá respecto de los menores. El consentimiento para tratar los datos de los menores lo otorgarán su padres o representantes legales así lo dispone el artículo 13 del Real Decreto 1720/2007, por el que se desarrolla la Ley Orgánica 15/1999 “Podrán tratarse los datos de los menores de catorce años con el consentimiento de padres o tutores.”
En el caso de obtenerse el consentimiento tanto del profesorado y quienes presenten servicio en el mismo, como de los menores las cámaras podrán instalarse, debiendo de informarse de la existencia de las mismas en los términos del artículo 5.1 de la Ley 15/1999, crear el oportuno fichero, que tendrá carácter público e inscribirlo en el Registro General de Protección de Datos, mediante la aprobación de la oportuna Disposición General que se publicará en el Diario Oficial Correspondiente, en los términos del artículo 20 de la Ley 15/1999, así como adoptar las medidas de seguridad de nivel básico que se recogen en la Ley Orgánica y se detallan en el Reglamento.

Informe 0317/2009 sobre: cesión de datos de minusvalía de alumnos entre Universidades públicas para estudio o investigación.

La consulta plantea si la Cátedra de Accesibilidad, Arquitectura y Diseño de la Universidad consultante puede solicitar a Universidades Públicas Españolas los datos de estudiantes con discapacidad matriculados en las mismas, con objeto de de contactar con ellos para la realización de un estudio en relación con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

I

La comunicación de datos de alumnos de otras Universidades que refiere la consultante constituye una cesión de datos en los términos que la define el artículo 3.i) de la LOPD: "Toda revelación de datos realizada a una persona distinta del interesado."

Los datos personales que solicitaría la consultante se circunscriben a los alumnos que tengan la condición de minusválidos, por lo que el dato de minusvalía nos situaría ante un tratamiento de datos de salud, definidos en el artículo 5 g) del Reglamento 1720/2007 que desarrolla la LOPD como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos al porcentaje de discapacidad y a su información genética." Es criterio de esta Agencia, ratificado por la jurisprudencia de lo contencioso-administrativo, que la minusvalía es un dato de salud..

En cuanto a la comunicación o cesión de datos de salud, es preciso indicar que la Ley Orgánica 15/1999 establece un régimen especial para su tratamiento y, en su caso, comunicación, considerándolos datos especialmente protegidos, debiendo plantearse si existe algún supuesto en que la propia Ley Orgánica da cobertura a esa cesión.

Como regla general, el artículo 7.3 de la Ley Orgánica 15/1999 dispone que "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente". Este artículo determina el contenido esencial del derecho fundamental a la protección de datos de carácter personal debido a su carácter orgánico.

La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección.

En este sentido, el artículo 8 de la Directiva 95/46/CE limita el tratamiento de datos a supuestos y finalidades concretos en los que será preciso el consentimiento, que además deberá ser expreso, del afectado o la necesidad del tratamiento con fines de asistencia sanitaria o atención de un interés vital del afectado. Esta cuestión ha sido especialmente analizada por el Grupo de Autoridades de Protección de Datos creado por el artículo 29 de la citada Directiva en su Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (Documento EP131), en el que se indica expresamente que "todos los datos contenidos en documentos médicos, en historiales médicos electrónicos y en sistemas de HME son "datos personales sensibles". Por tanto, no sólo están sujetos a todas las normas generales sobre protección de datos personales de la Directiva, sino

también a las normas sobre protección de datos especiales que rigen el tratamiento de la información sensible, contenidas en el artículo 8 de la Directiva".
Establecida ya por el artículo 7.3 la regla general del consentimiento expreso para el tratamiento de los datos de salud, el artículo 7.6 establece en su párrafo primero que "podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 (datos de salud) de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto". Igualmente, conforme al párrafo segundo del propio artículo 7.6, "También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".
Respecto de lo dispuesto en el artículo 7.6, el documento WP131 del Grupo creado por el artículo 29 de la Directiva 95/46/CE recuerda que "Puesto que el artículo 8, apartado 3, de la Directiva (que transpone el citado artículo 7.6)) constituye una excepción a la prohibición general de tratar datos sensibles, esta excepción deberá interpretarse de forma restrictiva". De este modo, señala que: "Esta excepción cubre solamente el tratamiento de datos personales para el propósito específico de proporcionar servicios relativos a la salud de carácter preventivo, de diagnóstico, terapéutico o de convalecencia, y a efectos de la gestión de estos servicios sanitarios."
No se cubre el tratamiento posterior que no sea necesario para la prestación directa de tales servicios. En el mismo sentido se pronuncia la SAN de 31-05-2002 al señalar " (…) La excepción del artículo 7.6 debe ser interpretada restrictivamente. Será preciso atender en cada caso concreto a que el tratamiento se dirija específicamente a la prevención y diagnóstico."
Por otra parte, el artículo 8 de la Ley Orgánica 15/1999 establece respecto a los datos de salud que "Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad".
Por último, el artículo 11.2 f) de la Ley Orgánica establece la licitud de la cesión de determinados datos relacionados con la salud si la misma es "necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".
La Agencia Española de Protección de Datos ha puesto reiteradamente de manifiesto que la aplicación del artículo 7.3 implica, por mor del principio de especialidad, la imposible aplicación a los datos referidos en el mismo de cualquiera de las causas legitimadoras del tratamiento previstas en el artículo 11.2 de la Ley Orgánica, quedando limitados los supuestos habilitantes del tratamiento y cesión de estos datos a los establecidos en la norma especial o a aquéllos en los que la norma general se refiere expresamente a tales datos (como sucede en relación con los datos de salud en el artículo 11.2 f) de la Ley Orgánica 15/1999).

II

El apartado segundo del artículo 11.2 de la LOPD contempla una serie de supuestos en que las cesiones de datos no requieren el consentimiento de los interesados, entre los que se encuentra, en lo que ahora interesa, el recogido en el apartado 2.e), esto es,

que la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
Analizando concretamente el supuesto esto es, que la cesión se efectúe para el tratamiento posterior de los datos con fines científicos, la cesión de datos entre Administraciones Públicas y en el seno de una misma Administración, tiene sin embargo un régimen específico establecido en el artículo 21 de la Ley Orgánica 15/1999, precepto que se ha visto afectado por la Sentencia del Tribunal Constitucional 292/2.000, de 30 de noviembre, indicando la redacción resultante de la anulación parcial del mismo como consecuencia de la comentada Sentencia que "los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".
Ello implicaría que tanto el cedente como el cesionario tuviesen encaje en el concepto jurídico de Administración Pública, supuesto que no plantea problemas en este caso, pues se trataría de una Universidad Pública que solicita los datos a otras Universidades Públicas.
En el supuesto objeto de consulta, desconocemos si el desarrollo de un estudio sobre la accesibilidad en las Universidades Públicas va a desarrollarse a titulo personal por una serie de investigadores o es un proyecto institucional a realizar en el marco de algún programa de investigación en concreto. Lo anterior es importante, a efectos de valorar si nos encontramos en presencia de un auténtico estudio científico y en consecuencia amparado por el supuesto de cesión contemplado en el artículo 11. 2 e) y 21. 1 de la Ley 15/1999, cuando aluden al fin científico del tratamiento de los datos personales como supuesto que al excluir el consentimiento previo a la cesión de los mismos.
En este sentido, el Titulo VII de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, dedicado a la investigación en la Universidad, considerándola como una función esencial de la Universidades, asumiendo como uno de sus objetivos el desarrollo de la investigación científica. A su vez, el artículo 40 regula la investigación como un derecho y un deber del profesorado universitario al establecer:
"1. La investigación es un derecho y un deber del personal docente e investigador de las Universidades, de acuerdo con los fines generales de la Universidad, y dentro de los límites establecidos por el ordenamiento jurídico.
2. La investigación, sin perjuicio de la libre creación y organización por las Universidades de las estructuras que, para su desarrollo, las mismas determinen y de la libre investigación individual se llevará a cabo, principalmente, en grupos de investigación, Departamentos e Institutos Universitarios de Investigación.
3. La actividad y dedicación investigadora y la contribución al desarrollo científico, tecnológico o artístico del personal docente e investigador de las Universidades será criterio relevante, atendida su oportuna evaluación, para determinar su eficiencia en el desarrollo de su actividad profesional.
4. Las Universidades fomentarán la movilidad de su personal docente e investigador, con el fin de mejorar su formación y actividad investigadora, a través de la concesión de los oportunos permisos y licencias, en el marco de la legislación estatal y autonómica aplicable y de acuerdo con las previsiones estatutarias consignadas al efecto."
A modo de conclusión, únicamente en el supuesto de que el trabajo que tiene como finalidad identificar las condiciones de accesibilidad y un análisis de la opinión de los estudiantes minusválidos al respecto, que puedan estar afectando a la salud de dichos alumnos, se desarrollase por el Departamento o Cátedra a título institucional y en el

marco de algún proyecto de investigación en concreto, podría ser de aplicación el artículo 21. 1 (y 11.2 e) de la Ley en lo que respecta a la cesión de datos que no guarden relación con la salud de los estudiantes, siendo en caso contrario (desarrollo del mismo a título personal por personal docente universitario, adscrito o no al mismo) de aplicación el artículo 11.1 Ley.

De acuerdo con el texto del artículo 4.2 de la Ley 15/1999, "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos". En el presente caso, con independencia de que se trate de un estudio realizado por la Universidad y para la misma, consideramos que la finalidad descrita sería incompatible con la finalidad que motivó su recogida, toda vez que los datos fueron recogidos y tratados para el adecuado cumplimiento de la relación jurídica existente entre la Universidad y quienes se matricularon en ella para recibir formación académica, sin que pueda considerarse, que dicha finalidad incluye, directa o indirectamente, la realización de los estudios que se plantean por lo que será preciso el consentimiento expreso de los afectados.

En el supuesto objeto de consulta, donde la cesión tendría una finalidad de estudio y desarrollo de un trabajo de investigación, no sería aplicable la excepción a dicho consentimiento establecida en el artículo 11. 2 f) que citábamos con anterioridad. Cabe así concluir que la cesión planteada, en cuanto contenga datos de salud, debe quedar sometida, al consentimiento expreso del interesado, con independencia de que el trabajo a desarrollar se inserte o no en el marco de un proyecto institucional.

Informe 0345/2009 sobre: La grabación por razones de seguridad en entornos escolares.

La consulta plantea si la instalación de cámaras que tienen en sus centros de enseñanza cumple con la legalidad vigente, esto es con la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
Según señala la consulta, la contestación que recibió de la Agencia Española de Protección de Datos, no satisfacía la consulta planteada, sin embargo debe puntearse que en su primer escrito de fecha 2 de abril del 2009 se solicitaba en letra mayúscula y negrita "QUE SE NOS CONCEDA AUTORIZACIÓN PARA LA INSTALCIÓN DE VIDEOCÁMARAS EN ESTE ÁMBITO Y LA GRABACIÓN DE LAS MISMAS EN AULAS Y PASILLOS DURANTE EL HORARIO DE CLASES."
Como en la súplica de su primer escrito requería "Autorización", la Agencia le contestó que no otorgaba ese tipo de autorizaciones y le explicaba sucintamente los requisitos para que las cámaras instaladas cumplan con la legalidad vigente.
En su segundo escrito, solicita aclaración sobre la legitimación para grabar a los alumnos menores de edad en sus centros, durante el horario escolar.
Del tenor de la consulta se desprende que la grabación de las imágenes se efectúa con la finalidad de controlar "hurtos o situaciones de acoso escolar" que se estaban produciendo en horario escolar, en definitiva se trata de instalar cámaras o videocámaras por motivos de seguridad.
Al tratarse de motivos de seguridad resulta de aplicación la Ley 23/1992, de 30 de julio de de Seguridad Privada, en la que se fundamenta la legitimación para grabar las imágenes tanto de los menores de edad como de aquellas personas que acudan al centro.
En cuanto a la legitimación para el tratamiento de las imágenes el artículo 2 de la Instrucción 1/2006, se remite a lo dispuesto en el artículo 6.1 y 2 de la Ley Orgánica de Protección de Datos, donde se establece que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa". El mencionado artículo debe de conectarse con lo dispuesto en la Ley 23/1992, de 30 de julio, de Seguridad Privada (en adelante LSP), que regula, según su artículo 1.1 "la prestación por personas, físicas o jurídicas, privadas de servicio de vigilancia y seguridad de personas o de bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de seguridad pública".
Asimismo, añade el artículo 1.2 que "A los efectos de la presente Ley, únicamente pueden realizar actividades de seguridad privada y prestar servicios de esta naturaleza las empresas de seguridad y el personal de seguridad privada, que estará integrado por los vigilantes de seguridad, los jefes de seguridad y los escoltas privados que trabajen en aquéllas, los guardas particulares del campo y los detectives privados",(..).
El artículo 5.1 e) de la LSP dispone que "Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollen, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades (…) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad". Esta previsión se reitera en el artículo 1 del Reglamento de Seguridad Privada, aprobado por Real decreto 2364/1994, de 9 de diciembre (en adelante RSP)
De este modo, la Ley habilitaría que los sujetos previstos en su ámbito de aplicación puedan instalar dispositivos de seguridad, entre los que podrían encontrarse las cámaras, siempre con la finalidad descrita en el citado artículo 1.1.

Para la efectiva puesta en funcionamiento de la medida, el artículo 6.1 dispone que "Los contratos de prestación de los distintos servicios de seguridad deberán en todo caso consignarse por escrito, con arreglo a modelo oficial, y comunicarse al Ministerio del Interior, con una antelación mínima de tres días a la iniciación de tales servicios".
El artículo 20 del RSP regula el procedimiento de notificación del contrato, la autoridad competente y el régimen aplicable a la contratación del servicio por las Administraciones Públicas y a supuestos excepcionales que exijan la inmediata puesta en funcionamiento del servicio.
Por último, el artículo 7.1 establece que "Para la prestación privada de servicios o actividades de seguridad, las empresas de seguridad habrán de obtener la oportuna autorización administrativa mediante su inscripción en un Registro que se llevará en el Ministerio del Interior".
La inscripción se regula en el artículo 2 del RSP, detallando el Anexo los requisitos que han de reunir estas empresas. No obstante, quedarían excluidas las de ámbito exclusivamente autonómico. Además, el artículo 39.1 dispone que "únicamente podrán realizar las operaciones de instalación y mantenimiento de sistemas de seguridad electrónica contra robo e intrusión y contra incendios las empresas autorizadas".
En consecuencia, siempre que se haya dado cumplimiento a los requisitos formales establecidos en los artículos precedentes (inscripción en el Registro de la empresa y comunicación del contrato al Ministerio del Interior), las empresas de seguridad reconocidas podrán instalar dispositivos de seguridad, entre los que se encontrarían los que tratasen imágenes con fines de videovigilancia, existiendo así una habilitación legal para el tratamiento de los datos resultantes de dicha instalación.
Así, quedaría legitimado por la existencia de una norma con rango de Ley habilitante el tratamiento al que se refiere el apartado 2 de los citados con anterioridad, siempre que se cumplan los requisitos a los que se ha hecho referencia o concurra una de las excepciones previstas en el RSP, no siendo necesario el consentimiento del afectado"
De este modo, el consultante deberá contratar con una empresa de seguridad que haya cumplido los requisitos antes expuestos, para que el tratamiento de las imágenes quedará legitimado, por la existencia de una norma con rango de Ley habilitante, no siendo por tanto necesario el consentimiento de los afectados.
Los requisitos que se acaban de exponer son aplicables cuando la finalidad de la grabación sea la seguridad, por el contrario si el tratamiento de las imágenes se efectúa con fines distintos a la seguridad será necesario obtener el consentimiento para legitimar el tratamiento.
Respecto del consentimiento de los menores de edad, el artículo 13 del Reglamento de desarrollo de la Ley Orgánica aprobado por Real Decreto 1720/2007, de 21 de diciembre regula el consentimiento para el tratamiento de datos de menores de edad, estableciendo que "1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.”

Informe 0477/2009 sobre: Medidas de seguridad aplicables al campus virtual de un centro escolar.

La consulta plantea que medidas de seguridad deben aplicarse al campus virtual de que dispone la consultante y en el que se introducen actas de evaluación, calificaciones, observaciones académicas, procesos y circunstancias concurrentes en los resultados finales de sus alumnos, así como un servicio de correo electrónico y mensajería.

Como cuestión previa, debe señalarse que la publicación de datos personales de los alumnos en la página web del colegio, esto es, cuando a ellos pueda acceder cualquier persona que consulte dicha página, constituye una cesión o comunicación de datos de carácter personal, definida por el artículo 3 j) de la LOPD como *"Toda revelación de datos realizada a una persona distinta del interesado".*

En relación con las cesiones de datos, prescribe el artículo 11.1 de la LOPD que *"Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".*

En consecuencia, la publicación de datos personales relativos a los alumnos, entre los que debe recordarse que están incluidas las imágenes, requiere el consentimiento informado, en los términos del artículo 5 de la Ley Orgánica 15/1999, del afectado o de sus padres si se trata de un menor de 14 años. A este respecto establece el número primero del artículo 13, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre que "*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores."*

En este mismo sentido, cabe señalar que el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo 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, en el Dictamen 2/2009, sobre la protección de los datos personales de los niños, en el que se contempla el especial supuesto de los colegios, recuerda, al referirse a los sitios web creados por éstos, que deben ser conscientes de que divulgar información personal justifica un cumplimiento más riguroso de los principios fundamentales de protección de datos. Igualmente recomienda que se pongan en marcha mecanismos de acceso restringido con vistas a proteger la información personal en cuestión, por ejemplo mediante la conexión con nombre de usuario y contraseña.

Asimismo, el aludido Dictamen advierte que debe prestarse una especial atención a la publicación por parte de los colegios de fotos de sus alumnos en Internet, debiendo hacerse siempre una evaluación del tipo de foto, la pertinencia de su publicación y su objetivo. Hace referencia a que incluso en aquellos casos en que se tomen fotografías colectivas que no permitan una fácil identificación de los alumnos, y que por tanto podrían no estar sujetas a la normativa de protección de datos, las escuelas deben informar a los niños y a sus padres de que se van a tomar fotografías y como van a utilizarse, dándoles la oportunidad de rehusar su inclusión en dicha foto.

Igualmente, debe recordarse que esta Agencia ha publicado unas recomendaciones para la protección de datos de los menores, en las que se señalaba que deben extremarse las precauciones en Internet y, en particular, se indicaba que "no es aconsejable publicar fotos que identifiquen a un niño, por ejemplo situándole en el contexto de un colegio y/o actividad determinados."

En cuanto a la concreta consulta formulada, relativa a la necesidad de cifrar los contenidos del Campus virtual, debe señalarse en primer lugar que el artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece en sus números primero y segundo 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 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 estén 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."

Por su parte el número tercero de la Disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, dispone que *"En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo."*

El Reglamento de desarrollo de la Ley Orgánica 15/1999, al que antes se ha hecho referencia, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

En cuanto a la determinación del nivel aplicable en cada caso dispone el artículo 81 del Reglamento:

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los relativos a la comisión de infracciones administrativas o penales.

b. *Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.*

c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c. *Aquéllos que contengan datos derivados de actos de violencia de género."*
A la vista de los contenidos del campus virtual indicados en la propia consulta, deberán adoptarse las medidas de nivel medio, por aplicación del apartado 2.f) del artículo 81 transcrito, salvo en el caso de que se incluyan, además, datos relativos a salud, religión o algún otro dato de aquellos a los que hace referencia el número 3 del artículo 81, en cuyo caso sería preciso adoptar las medidas de seguridad de nivel alto.
En lo que se refiere al acceso a datos a través de redes de comunicaciones el artículo 85 prevé que *"Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80."*
De esta manera, teniendo en cuenta, que como se ha señalado, la aplicación de las medidas de nivel medio exige la aplicación de las de nivel básico, el artículo 91 del Reglamento impone en los ficheros de nivel básico como primera medida de seguridad la del control de acceso, disponiendo en su número primero que "*Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones",* para ello exige en su número tercero que *"El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados."* Debe entenderse en el presente supuesto que los usuarios, en este caso los padres de los alumnos, tendrán acceso exclusivamente a los datos de sus hijos, ya que en otro caso estaríamos ante una cesión de datos que requeriría el consentimiento de los afectados como ya se ha indicado.
Asimismo, establece una obligación de identificación y autenticación de los usuarios, exigiéndose ya desde el nivel básico una identificación personalizada de los usuarios, a diferencia de la normativa anterior en la que tenían cabida los usuarios genéricos. Dispone el artículo 93.1, a estos efectos, que "*El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios*." Por su parte, el número 2 del mismo artículo prevé que "*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."*
En el nivel medio, esta medida de identificación y autenticación se vuelve más rigurosa ya que, a las medidas anteriores previstas para el nivel básico, se añade la contenida en el artículo 98 según el cual "*El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información."* Por último, en el nivel alto, se requiere ya un registro de cada intento de acceso que se produzca, establece el artículo 103.1 que "*De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado*." Mientras que el número segundo del mismo artículo dispone "*En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido."* En lo que se refiere a la medida de cifrado de datos, solamente es exigida en el supuesto previsto en el artículo 104, según el cual *"Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros."*

Por consiguiente, la normativa de protección de datos solamente exige el cifrado de los datos cuando éstos, por su naturaleza, estén sujetos a medidas de seguridad de nivel alto, y ello sin perjuicio de que, conforme a lo previsto en el artículo 81.8 del mismo Reglamento, pueda segregarse el fichero, aplicando las medidas de seguridad de nivel alto únicamente a los datos de tal carácter. Así dispone dicho artículo que "*A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.*"

No obstante, debe recordarse que el artículo 81.7 del Reglamento dispone que "*Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero*." En consecuencia, la medida de cifrado de los datos puede ser adoptada voluntariamente por el responsable del fichero.

Informe 0572/2009 sobre: Medidas de seguridad a adoptar para los ficheros con datos académicos.

Se consulta el nivel de medidas de seguridad a aplicar a un fichero que incorpora diversos datos personales de alumnos, entre ellos, además de los identificativos, los relativos a edad, sexo, nacionalidad, titulaciones, historial académico, formación, seguimiento y calificaciones académicas y evaluación del nivel académico.
El 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, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.
El artículo 81 del citado Reglamento dispone respecto de la aplicación de los niveles de seguridad lo siguiente:
"1. *Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.*
2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:
a. Los relativos a la comisión de infracciones administrativas o penales.
b. *Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.*
c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.
f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:
a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c. *Aquéllos que contengan datos derivados de actos de violencia de género."*
Esta Agencia ha venido señalando respecto a la interpretación que debe darse al artículo 81.2.f) que de dicho precepto se desprende que su finalidad es someter a criterios de seguridad más rigurosos aquellos ficheros que permitan obtener una información adicional sobre el afectado, a partir de los datos que en los mismos se incluyen, obteniendo así un perfil de su situación económica o familiar o de sus aficiones, hábitos de compra o preferencias, entre otros aspectos.

Así, se encontrarán comprendidos en el artículo 81.2 f) todos los ficheros que contengan datos a partir de los cuales puedan deducirse cualquiera de las facetas antes mencionadas o, como sucede en el presente caso, se incluyan datos relativos al rendimiento académico y curriculares que permitan deducir un perfil de estudios, de modo que el nivel de medidas de seguridad aplicable al supuesto consultado será el medio, debiendo también aplicarse las medidas de nivel básico, toda vez que los niveles son acumulativos.

No obstante, debe indicarse que si el fichero contuviera datos referentes al perfil psicológico de los afectados y que hicieran referencia a la existencia de anomalías o especialidades de la personalidad del sujeto, habrá de considerarse que el fichero contiene datos relacionados con la salud de las personas, siendo entonces de aplicación lo dispuesto en el artículo 81.3 a) del reglamento, que exige la adopción sobre estos ficheros de las medidas de seguridad de nivel alto, además de las medidas de nivel básico y medio.

Informe 0037/2010 sobre: Datos disociados – notas de selectividad agregadas por colegios.

La consulta plantea si resulta conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal la solicitud a los centros docentes de Andalucía de determinadas informaciones referidas a los alumnos presentados por cada centro a las pruebas de acceso a laUniversidad, la nota media de sus expedientes y de la prueba de selectividad.

Según se indica únicamente será solicitada información agregada referida al número de alumnos en total y a las notas medias de los mismos, sin que dicha información sea objeto de desglose alguno.

Conforme establece el artículo 2.3 de la Ley Orgánica, "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", siendo datos de carácter personal, conforme al artículo 3 a), "Cualquier información concerniente a personas físicas identificadas o identificables".

Frente a este concepto se contrapone el de dato disociado, contenido em el artículo 5.1 e) del Reglamento de desarrollo de la Ley Orgánica, aprobado por Real decreto 1720/2007, de 21 de diciembre, como "aquél que no permite la identificación de un afectado o interesado". En consecuencia, serían disociados los datos no referidos a una persona identificable, señalando el artículo 5.1 o) del propio Reglamento que es identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados".

En resumen, cuando el tratamiento se refiere únicamente a datos disociados que no permiten identificar al afectado al que los mismos se refiere no nos encontraremos ante datos de carácter personal y, en consecuencia, no estaremos dentro del ámbito descrito en el artículo 2.1 de la Ley Orgánica 15/1999. EN este sentido, recuerda, a título de ejemplo, el artículo 11.6 de la Ley Orgánica, para el supuesto de cesión o comunicación de datos que "Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores".

De lo que se indica en la consulta se desprende que la consultante únicamente va a proceder al tratamiento de los datos identificativos del centro de enseñanza así como de los relativos al número de alumnos presentados a las pruebas de acceso a la Universidad y número de alumnos presentados en cada convocatoria con indicación de la media total de sus expedientes y de la puntuación obtenida en la prueba.

A la vista de esta información, y en los términos que se han indicado, la consultante únicamente trataría datos disociados, no siendo aplicable al tratamiento lo previsto en la Ley Orgánica 15/1999 y su normativa de desarrollo.

Informe 0179/2010 sobre: La creación de direcciones de correo a alumnos menores de edad – legitimación para el tratamiento

I

La consulta plantea, en primer lugar, si resulta necesario el consentimiento de los padres de alumnos de edades que podrían llegar a un mínimo de diez años de edad para la creación a los mismos de una cuenta de correo electrónico en el marco de la implantación e un programa "que impulsa el empleo de las nuevas tecnologías en las aulas".

Como punto de partida, debe indicarse que la legislación de protección de datos no resulta en sí misma aplicable de modo directo a la creación de una cuenta de correo electrónico. No obstante, dicha creación y el uso de dicha cuenta implicará el tratamiento por parte del prestador de ese servicio de los datos de carácter personal del usuario, lo que hace que sí hayan de ser tenidas en cuenta las mencionadas normas.

Dicho esto, si se parte del hecho de que el Programa es de implantación necesaria en el ámbito de la administración educativa de la Comunidad Autónoma, sería preciso tener en cuenta que el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, dispone que "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa", añadiendo el artículo 6.2 que dicho consentimiento no será preciso cuando los datos "se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

Teniendo esto en cuenta, de los escuetos términos de la consulta parece desprenderse que es uno de los objetivos del programa la implantación del uso de las nuevas tecnologías en el ámbito escolar, siendo así necesario para un verdadero cumplimiento de dicho objetivo la creación de las mencionadas cuentas, por lo que podría entenderse que el tratamiento resulta necesario para el adecuado desarrollo de la relación jurídica que vincula al alumno con el centro escolar, no siendo así necesario su consentimiento para el tratamiento de tales datos.

Ahora bien, la conclusión que acaba de alcanzarse legitimaría el tratamiento en el supuesto en que los datos referidos a la atribución y el empleo de la relación de correo electrónico se lleven exclusivamente a cabo para el adecuado mantenimiento o cumplimiento de la relación que vincula al alumno con el centro. De este modo, debería recaer sobre el propio centro o sobre la administración educativa de la Comunidad Autónoma la responsabilidad por el mencionado tratamiento, que sólo podría llevarse a cabo para el cumplimiento de los fines que se han venido describiendo y que se encuentran directamente vinculados a las competencias de la Administración educativa y del centro al que asista el menor.

Lo que acaba de indicarse resulta especialmente relevante si se tiene en cuenta el hecho de que la consulta plantea la posible apertura de cuentas de correo electrónico referidas a determinados "proveedores de este tipo de servicios".

Atendiendo a lo que acaba de indicarse, para que ello sea posible, los mencionados proveedores deberían mantener en relación con el tratamiento de datos derivados de la apertura de cuentas de correo la condición de encargado del tratamiento, siendo de aplicación a los mismos el régimen establecido en el artículo 12 de la Ley Orgánica 15/1999 y en la Sección Tercera del Capítulo II de su Reglamento de desarrollo, aprobado por Real decreto 1720/2007, de 21 de diciembre.

En particular, debe recordarse que, conforme dispone el artículo 12.2 de la Ley Orgánica "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita

acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas", añadiendo el precepto que "En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

Asimismo, el artículo 12.4 dispone que "En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personal".

La cuestión se plantea por el hecho de que las condiciones generales de privacidad de los proveedores de estos servicios, y en particular de los que se citan en la consulta, suelen implicar el tratamiento de datos de los titulares de las cuentas para determinadas finalidades que en ningún caso podrían encajar entre las que justificarían el tratamiento de los datos sin consentimiento de los mencionados titulares, pudiendo en particular hacerse referencia al posible uso de los datos para finalidades relacionadas con la remisión publicitaria asociada al correo recibido o enviado.

De este modo, en tanto los proveedores del servicio empleasen los datos para estas finalidades, su posición jurídica no podría ser la de encargado del tratamiento, generándose una relación directa entre aquéllos y el interesado que otorgaría a los mismos la condición de responsable, tal y como determina el artículo 20.1, párrafo último, del Reglamento de desarrollo de la Ley Orgánica 15/1999, así como el ya citado artículo 12.4 de la Ley Orgánica 15/1999.

Ello sí exigiría que los interesados debieran prestar su consentimiento para el tratamiento de sus datos asociados a la creación de la cuenta de correo electrónico, en lo que se refiere a cualquier uso de los datos que excediera de la relación entre el alumno y el Centro o la Administración Educativa, procediendo la aplicación de las normas legales y reglamentarias relativas a la prestación del mencionado consentimiento.

En particular, dado que la consulta se refiere a alumnos que podrían tener la edad de diez años, debería tenerse en cuenta que conforme al artículo 13.1 del Reglamento "Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores".

De este modo, sí podría resultar necesario el mencionado consentimiento de los padres o tutores del menor en caso de que el servicio sea prestado por un proveedor de servicios de Internet que no fuera a limitar su actuación a la mera prestación del servicio a la Administración autonómica.

Por todo ello, y en relación con esta primera cuestión, sería conveniente que las direcciones fueran otorgadas por la propia Administración autonómica y no atribuidas en relación con un prestador de servicios de la sociedad de la información cuya política de privacidad implique el tratamiento de datos que excede de la finalidad pretendida, no resultando necesario, en caso de atribuirse las cuentas directamente por la Administración, el consentimiento del interesado ni de sus representantes legales.

II

En segundo lugar, la consulta plantea quién será responsable del tratamiento en relación con el uso por los centros privados y concertados de una aplicación informática, alojada en los servidores de la Administración autonómica, con distintos grados de acceso en virtud del colectivo afectado y en que se incluyen datos relacionados con distintas cuestiones.

Ante todo, es preciso indicar que los términos de la consulta no permiten analizar detenidamente el funcionamiento o las funcionalidades de la aplicación, ni los grados o rangos de acceso a la misma. Asimismo, se desconoce si la aplicación implica el acceso y uso de los datos por parte de la propia administración educativa autonómica o si en la práctica se está únicamente haciendo referencia a la creación por dicha administración de una aplicación que podrá ser empleada por los centros, incluso con carácter preceptivo en relación con los de titularidad pública y los concertados.
No obstante, de los términos de la consulta parece, efectivamente, desprenderse que nos encontramos simplemente ante la creación y alojamiento de la mencionada aplicación, que será directamente empleada en el ámbito de cada uno de los centros.
En ese caso, sería aplicable la doctrina ya sostenida por la Agencia en relación con casos similares, pudiendo hacerse referencia al informe de 16 de junio de 2008, en que se señalaba, con expresa referencia a la normativa aplicable a dicha Comunidad, que debería analizarse para el caso de la ahora consultante, lo siguiente:
"La Orden de 20 de julio de 2006, de la Consejería de Educación de Andalucía, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de los sistema SÉNECA y PASEN, señala en su Anexo I que dichos sistemas "proporcionan la infraestructura técnica para el manejo de la información académica y de gestión de los centros educativos dependientes de la Consejería de Educación de la Junta de Andalucía", añadiendo que "esto incluye a los centros educativos de carácter público de la Comunidad y a los centros educativos concertados que utilizan estos sistemas para el soporte de determinados procesos de gestión". En consecuencia, debe diferenciarse entre los ficheros de datos regulados por la citada Orden y los propios sistemas SÉNECA y PASEN, definidos por el propio texto como herramientas de manejo de la información y gestión académica de los centros integrados en el sistema educativo público de la Comunidad Autónoma. En este sentido, el artículo 3.1 de la Ley 17/2007, de 10 de diciembre, de Educación de Andalucía establece que "el Sistema Educativo Público de Andalucía es el conjunto de centros, servicios, programas y actividades de las administraciones públicas de la Comunidad Autónoma o vinculados a las mismas, orientados a garantizar el derecho de la ciudadanía a una educación permanente y de carácter compensatorio, reconocido en el artículo 21.1 del Estatuto de Autonomía para Andalucía", añadiendo el apartado 3 que el Sistema está compuesto por los centros docentes públicos de titularidad de la Junta de Andalucía o de las Corporaciones Locales u otras Administraciones Públicas, así como por los centros docentes privados concertados, sin perjuicio de la legislación específica que pudiera resultar de aplicación a los mismos. Dentro del ámbito competencial de la mencionada Comunidad Autónoma, la Ley 17/2007 contiene en su Título V determinadas previsiones tendentes a uniformar la gestión de los procesos automatizados de datos por parte de los centros integrados en el Sistema Público. Así, el artículo 142.1 dispone que "la Administración educativa favorecerá el funcionamiento en red de los centros educativos, con objeto de compartir recursos, experiencias e iniciativas y desarrollar programas de intercambio de alumnado y profesorado". Por su parte, conforme al artículo 151 "La Administración educativa facilitará e impulsará la realización de trámites administrativos a través de Internet, así como la relación electrónica de la ciudadanía con los centros docentes. A tales efectos, se prestará especial atención a los procedimientos de escolarización y matriculación del alumnado, así como a los que realizan los miembros de la comunidad educativa, particularmente el profesorado".
De lo dispuesto en la Orden de creación de ficheros y la Ley 17/2007 se desprende, como se ha venido indicando que los sistemas SÉNECA y PASEN se configuran como herramientas encaminadas a facilitar y agilizar los trámites relacionados con la gestión de los centros integrados en el Sistema Educativo Público de Andalucía, debiendo en

consecuencia diferenciarse entre el propio sistema, como aplicación puesta a disposición de los Centros por la Administración Autonómica, en desarrollo de los artículos 142.1 y 151 de la Ley, de los propios ficheros previstos en la Orden o aquellos de los que en uso de la aplicación sean creados y gestionados por los centros integrados en el sistema. De este modo, la situación es en principio similar a la de los sistemas de información existentes en otras áreas de actividad cuya competencia corresponda al sector público. Así, en principio, no cabría apreciar diferencia entre los sistemas analizados y otros que fueran desarrollados, por ejemplo, para la gestión de las historias clínicas en el ámbito del Sistema sanitario de una determinada Comunidad Autónoma o los que fueran desarrollados por un determinado departamento para la gestión de recursos humanos o la gestión presupuestaria de los restantes Departamentos integrantes de dicha Administración.

Consecuencia de lo que acaba de indicarse es que los Centros concertados, dotados de personalidad enteramente independiente de la Administración educativa autonómica serán responsables de los ficheros relacionados con la utilización de la herramienta o sistema informático puesto a su disposición, siendo tales ficheros diferentes de los creados expresamente para el ámbito de la Administración Pública por su propia Orden de creación."

La conclusión mantenida en el citado informe sería igualmente extrapolable a los centros privados, que ostentarían igualmente la condición de responsable del tratamiento.

Asimismo, y teniendo en cuenta que la consulta indica que la aplicación se alojaría en los propios servidores de la Comunidad Autónoma, la misma actuaría en relación con el uso de la aplicación por los centros privados y concertados como encargada del tratamiento, debiendo dar cumplimiento a lo dispuesto en el artículo 12 de la Ley Orgánica y en los artículos 20 a 22 de su Reglamento de desarrollo.

II - CONSULTAS FRECUENTES SOBRE LA PROTECCIÓN DE DATOS EN EL ÁREA DE LA EDUCACIÓN (apdm)

I - Declaración de ficheros

¿Qué ficheros deben declarar los centros públicos de enseñanza de la Comunidad de Madrid, y cómo se declaran?

¿Sobre qué tipo de Ficheros de Carácter Personal ejerce sus funciones la Agencia de Protección de Datos de la Comunidad de Madrid?

¿Quién es el responsable de los ficheros que se utilizan en los centros públicos de enseñanza?

¿Pueden crearse y utilizarse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición en la que se crean?

¿Es obligatoria la declaración por parte de la Consejería de Educación de la Comunidad de Madrid de los ficheros con datos personales de la Escuelas Infantiles y casas de Niños, cuando dichos centros son gestionados por empresas privadas a través de un contrato de gestión de servicios público, o directamente por los Ayuntamientos?

¿Puede la Real Escuela Superior de Arte Dramático crear un fichero de datos de carácter personal sobre currículos y publicar los datos obrantes en él en la página Web de la citada Real Escuela?

¿Incluir en un fichero ya declarado de un Centro Educativo nuevos datos personales conlleva la creación de un nuevo fichero?

¿En relación con la protección de datos de carácter personal, cuáles son las características principales del Registro de Historiales Académicos y de Alumnado Escolarizado en la Comunidad de Madrid? ¿Y del procedimiento telemático para su gestión?

II - Derechos de los ciudadanos

¿Tiene la APDCM datos de carácter personal de los alumnos y/o profesores? ¿Y de los ciudadanos en general?

¿Cómo se puede dar cumplimiento al deber de información al interesado, que establece la LOPD, con carácter previo a la recogida de sus datos?

¿Cuándo cumplen con los términos del artículo 5 de la LOPD los impresos de los Centros Educativos utilizados para la recogida de datos de los alumnos? ¿Qué información ha de incluirse en los impresos por los que se solicita la concesión de la hipoteca joven de la Comunidad de Madrid?

¿Cómo puede un alumno o un profesor conocer la información que de él mismo tiene su Centro Educativo? ¿Para ejercitar su derecho de acceso es suficiente que acompañe una copia de su DNI?

¿Es posible denegar el ejercicio del derecho de acceso que la LOPD reconoce a los alumnos y/o profesores por la dificultad o el elevado coste que puede suponer su ejercicio?

¿Es conforme con la LOPD que un profesor cuyos datos están siendo objeto de tratamiento con motivo de su participación en un proceso selectivo que aún no ha concluido ejercite su derecho de acceso a los datos obrantes en un fichero sobre "Opositores Docentes"?

¿Vulnera la LOPD el hecho de tomar fotografías de alumnos en centros escolares?

III - Calidad de datos.

¿Qué datos pueden recogerse de los alumnos y/o de los profesores para el ejercicio de una determinada actividad por parte de un Centro Educativo?

¿Los datos recogidos para una determinada finalidad pueden utilizarse para cualquier otra que se pueda plantear a posteriori?

¿Puede cualquier empleado de un centro público de enseñanza acceder a los datos de carácter personal contenidos en los ficheros?

¿Puede utilizarse el dato del teléfono móvil de los alumnos, de los padres o de los profesores para la remisión de mensajes de texto vía SMS?

IV - Cesión de datos

IV – 1 - Cesiones de datos de los alumnos de los Centros Educativos

¿Las calificaciones académicas de los alumnos de un Centro Educativo pueden publicarse en los tablones o en Internet?

¿Cuáles son las fórmulas legales de publicación de los resultados de los siguientes procesos: Prueba de Acceso a estudios universitarios (Selectividad), Prueba de Acceso a la Universidad de los Mayores de 25 años y Proceso de Ingreso?

¿Es posible publicar en la página Web los datos que figuran en el acta de calificación de la convocatoria de los premios extraordinarios de bachillerato que otorga anualmente la Comunidad de Madrid?

¿Puede un profesor acceder al expediente académico de un alumno?

¿Puede repartirse entre los miembros del Consejo Escolar las notas de todos los alumnos con sus nombres para analizar sus dificultades específicas e impulsar las mejoras necesarias?

¿Los padres y tutores de los alumnos tienen derecho a solicitar las calificaciones académicas del Centro Educativo?

¿Podría la policía local acceder a los datos de menores escolarizados en un Centro educativo?

¿Conforme a la LOPD, podría la policía local acceder a los datos de los menores obrantes en un centro educativo para valorar las situaciones de desamparo o cualquier otra situación de riesgo del menor?

¿Sería conforme a la LOPD que un centro educativo elaborase un informe a petición de la Policía Local para valorar la situación socio-familiar del menor en supuestos tales como el de desamparo o en relación con cualquier otra situación de riesgo?

¿Es posible que un centro educativo público facilite a la Asociación de Madres y Padres de Alumnos del Centro (AMPA) los datos personales de los alumnos cuyos padres no son socios de la misma?

¿Es legítimo el acceso a los informes de Evaluación Pedagógica de los hijos por parte de los padres separados? En su caso, ¿es necesario informar de la solicitud recibida de uno de los padres al otro que tenga la guardia y custodia del hijo?

¿Pueden cederse datos de alumnos inmigrantes para realizar un seguimiento de vacunación de la población residente en la Comunidad de Madrid?

¿Es conforme con la LOPD que se informe a los profesores de un Centro Educativo afectados por riesgos para su integridad física y su salud de que un alumno del centro educativo es portador de una grave enfermedad de carácter contagioso?

¿Es conforme con la LOPD que la Administración educativa requiera la cumplimentación de determinados datos de carácter personal correspondientes a los alumnos de un Centro Educativo relativos a la circunstancia de ser gitano? En caso afirmativo ¿De qué modo debe procederse para confirmar que una persona determinada es de raza gitana? ¿Resulta conforme con la normativa sobre protección de datos la petición de documentación acreditativa de dicha pertenencia étnica y/o racial? ¿En el supuesto de menores de edad, el dato correspondiente debe recabarse del propio menor o de sus padres o tutores?

¿Resulta conforme con lo dispuesto en la LOPD el tratamiento de los datos de salud de los alumnos con discapacidad para llevar a cabo las correspondientes "adaptaciones curriculares", sin recabar para ello el consentimiento de los alumnos, padres o tutores?

¿Es conforme con la LOPD la solicitud de la Secretaría General Técnica de la Consejería de Educación a los centros docentes públicos y privados de determinados datos personales de alumnos graduados en un determinado curso en las enseñanzas de Educación Secundaria y de Formación Profesional, y de alumnos que abandonaron la ESO?

¿Conforme a la LOPD qué tipo de acceso a documentación con datos personales deberán tener los equipos de orientación educativa y psicopedagógica?

¿Resultaría conforme con la LOPD que se comunicase por el Centro de Educación de Personas Adultas de una Mancomunidad a un Ayuntamiento la

identificación de un alumno, menor de edad, causante de un determinado deterioro en el mobiliario de las aulas de un Centro educativo cuya titularidad pertenece a dicho Ayuntamiento?
¿Es necesaria la autorización del afectado o de su representante legal para el intercambio de fotografías de los alumnos en un determinado proyecto educativo? ¿Y para publicar fotografías e imágenes de los estudiantes en Internet?

¿Es posible el acceso a los datos de alumnos matriculados en el último curso de formación profesional en los centros educativos de la Comunidad de Madrid por parte de una empresa privada para llevar a cabo un estudio estadístico sobre formación profesional para el Consejo Superior de Cámaras?

¿Un Colegio Profesional puede tener acceso anual al listado de alumnos aprobados en el último curso del centro de estudio de la profesión en cuestión para enviarles información colegial necesaria para que puedan incorporarse al mundo laboral de ese sector?

IV – 2 - Cesiones de datos del personal de los Centros Educativos

¿Qué datos de los empleados públicos se pueden facilitar a los Delegados de Prevención del Comité de Seguridad y Salud de un Centro Educativo con el objeto de que se puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores para valorar sus causas y proponer las medidas oportunas?

El Comité de empresa o el Delegado de personal de un Centro Educativo han solicitado un listado nominativo de todos los empleados. ¿Cuáles son los datos que pueden entregarse a los representantes sindicales?

¿Pueden los representantes sindicales solicitar datos de los profesores en relación con el horario de los mismos? ¿Y sobre los datos relativos a profesores afectados por absentismo laboral?

¿Pueden ser cedidos por parte de la Dirección General de Recursos Humanos de la Consejería de Educación los datos referentes al número de puestos de trabajo, las titulaciones y nivel de estudios realizados, edades y adaptación de funciones de puestos de trabajadores con número de puesto de trabajo de las categorías a extinguir del personal laboral a una organización sindical?

¿Es conforme con la normativa sobre protección de datos la entrega al Comité de Empresa de Centros Educativos de la Relación de Puestos de Trabajo de dichos Centros, con detalle del centro de trabajo, nombre de los trabajadores de cada centro, categoría profesional de los trabajadores, número de puesto que cada uno ocupa, turno y horario de cada uno, tipo de contrato de cada trabajador, antigüedad y número de vacantes de cada centro?

¿Se pueden facilitar a las Centrales Sindicales promotoras de las elecciones a la Junta de Personal Docente datos personales de los funcionarios docentes electores, a los efectos de realizar un envío de propaganda electoral?

¿Puede publicarse en el tablón del Departamento correspondiente de un Instituto de Enseñanza Secundaria la hoja del horario individual de un profesor

incluyendo los datos personales de dirección personal, DNI, número de teléfono, fecha de nacimiento, antigüedad en el cuerpo y número de registro personal? ¿Y sus faltas de asistencia?
¿Puede un Instituto de Educación Secundaria publicar en la página Web del Centro el nombre de los profesores que imparten enseñanzas y el horario de atención a las consultas de los padres?

¿Se puede publicar en Internet el directorio: nombres y datos profesionales de contacto de todo el personal de un Centro Educativo?

¿Se pueden obtener datos de los profesores del fichero de gestión de personal docente a los efectos de enviar información sobre las convocatorias de cursos para la formación del profesorado dependiente de la Consejería de Educación?

¿Puede un centro docente de la Comunidad de Madrid ceder datos de los profesionales no funcionarios a un Colegio Oficial de la Comunidad de Madrid?

IV – 3 - Cesiones de datos derivadas de otras actuaciones en el ámbito educativo

¿Pueden publicarse en la página Web de la Consejería de Educación los listados de los participantes en procesos selectivos que tengan lugar?

¿Cómo debe procederse en la publicación de los datos personales de los alumnos beneficiarios y excluidos en la Convocatoria de ayudas de libros de texto y material didáctico?

¿Cómo debe procederse en la publicación de los datos personales de los alumnos beneficiarios y excluidos en la Convocatoria de ayudas de comedor escolar?

¿Debe un Centro Educativo de la Comunidad de Madrid entregar copia de un expediente al Defensor del Pueblo cuando esta institución lo demande? ¿Y al Defensor del Menor?

¿Se puede facilitar por parte del un Organismo Autónomo la documentación de los expedientes completos de las subvenciones que le han sido solicitadas a un diputado de la Asamblea de Madrid?

¿Puede intercambiarse información entre los Equipos de Orientación Educativos y los Equipos de Salud Mental?

¿Pueden cederse por el Instituto Madrileños del Menor y la Familia datos de personas que habían pertenecido al Sistema de Protección de la Comunidad de Madrid a la Consejería de Educación para la realización de una investigación?

¿Es conforme a la LOPD la solicitud por parte de la Concejalía de Educación de un Ayuntamiento a una Escuela Infantil del Municipio de una relación de familias pertenecientes a dicha Escuela, así como su domicilio postal, para presentar el Programa denominado "AMPLÍA"?

¿Resulta conforme con lo dispuesto en la normativa sobre protección de datos la utilización por parte de los alumnos de un Centro Educativo de una plataforma de Internet para realizar cursos on-line?

¿Puede imputarse a un Centro Escolar la vulneración de la privacidad de los datos personales de un alumno si un grupo de padres de los alumnos remite a otro padre, madre o tutor, un escrito -a su domicilio- recordándole la deuda que voluntariamente adquirió para material escolar, sin que el Colegio interviniera en tal acuerdo?

¿Qué requisitos hay que cumplir para poder entregar datos personales a entidades bancarias y cajas de ahorros para gestionar pagos y cobros del Centro Educativo?

V - Medidas de seguridad

¿Todos los ficheros que contengan datos de carácter personal deben cumplir las mismas medidas de seguridad?

¿Quién debe ser el responsable de seguridad?

¿Es necesario presentar ante la Agencia de Protección de Datos el Documento de Seguridad de los ficheros automatizados de datos de carácter personal?

¿Se puede cifrar el nombre y apellidos de los posibles adjudicatarios de plazas de Educación de Adultos en los Centros Penitenciarios mediante el sistema de concurso de traslados?

¿Qué medidas de seguridad deben aplicarse a un fichero de datos personales informatizado con datos especialmente protegidos ubicado en un único ordenador personal?

¿Cómo debe interpretarse el control de acceso físico?

Los centros educativos de titularidad pública en el ámbito de la Comunidad de Madrid pueden dirigirse a la Agencia de Protección de Datos de la Comunidad de Madrid para plantear preguntas relacionadas con la interpretación de la legislación vigente en protección de datos personales (ver apartado 3 de esta guía).

En el sitio Web de la APDCM (www.apdcm.es) se encuentra una sección con las consultas más frecuentes realizadas por los centros educativos de la Comunidad de Madrid, de entre las que hemos pretendido extractar algunas de las más significativas:

Declaración de ficheros

¿Qué ficheros deben declarar los centros públicos de enseñanza de la Comunidad de Madrid, y cómo se declaran?

Deben declararse todos aquellos ficheros que contengan datos de carácter personal, tanto si son informatizados, manuales estructurados, o mixtos (ficheros cuya información está en parte informatizada, en parte en soporte papel estructurado), siempre que estén identificadas o sean identificables las personas titulares de los datos.

El procedimiento para declarar ficheros está descrito con detalle en esta publicación.

¿Sobre qué tipo de Ficheros de Carácter Personal ejerce sus funciones la Agencia de Protección de Datos de la Comunidad de Madrid?

La Agencia de Protección de Datos de la Comunidad de Madrid ejerce sus funciones de control sobre los ficheros de datos de carácter personal creados o gestionados por:
- Los Órganos, Organismos, Entidades de Derecho público y demás Entes públicos que integran la Administración Pública de la Comunidad de Madrid.
- Los Entes integrantes de la Administración Local de la Comunidad de Madrid.
- Las Universidades Públicas.
- Las Corporaciones de derecho público representativas de intereses económicos y profesionales de la Comunidad, siempre que se creen para el ejercicio de potestades de derecho público.

¿Quién es el responsable de los ficheros que se utilizan en los centros públicos de enseñanza?

La LOPD define al responsable de los ficheros de datos personales como la persona física y jurídica que puede decidir sobre el contenido, la finalidad y uso de los datos.
En el caso de centros públicos de enseñanza el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia, teniendo capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza.

Por ejemplo, la responsabilidad sobre el fichero de alumnos de un colegio público corresponderá a la Dirección del centro en cuestión. El fichero de personal docente y el de personal de administración y servicios del centro serían responsabilidad de la Dirección General de Recursos Humanos de la Consejería de Educación. Todo ello sin perjuicio de los ficheros de profesores y personal de administración y servicios que estén adscritos a un determinado centro, cuya finalidad sea la gestión interna, de los cuales sería también responsable la Dirección del centro.

El responsable de un fichero debe indicarse expresamente en el correspondiente Anexo de la disposición a través de la cual se crea el mismo.

¿Pueden crearse y utilizarse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición en la que se crean?

No se puede llevar a cabo la creación y utilización de ficheros de datos de carácter personal por centros públicos de enseñanza sin la oportuna publicación de una disposición de carácter general. En este sentido la LOPD tipifica como infracción grave proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente.

De igual manera, la LOPD tipifica como infracción leve, cuando no sea constitutivo de infracción grave no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

¿Es obligatoria la declaración por parte de la Consejería de Educación de la Comunidad de Madrid de los ficheros con datos personales de la Escuelas Infantiles y casas de Niños, cuando dichos centros son gestionados por empresas privadas a través de un contrato de gestión de servicios público, o directamente por los Ayuntamientos?

Teniendo en cuenta que el responsable del fichero es la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, habrá que analizar en cada caso concreto quién es el responsable de los ficheros.

Cuando las Escuelas Infantiles y Casas de Niños se gestionen directamente por Centros Públicos dependientes de la Comunidad de Madrid a través de la Consejería de Educación, los responsables de los ficheros serán cada uno de esos centros públicos, siendo necesario, en la medida que se trata de Administración Pública, la aprobación de creación de dichos ficheros mediante la correspondiente Orden de la Consejería de Educación.

Una situación similar a la anterior se puede plantear cuando las Escuelas Infantiles y Casas de Niños sean gestionadas directamente por los Ayuntamientos de la Comunidad de Madrid, variando únicamente en ese caso, el tipo de disposición de carácter general que se dicte, dado que en ese supuesto será necesario que los Ayuntamientos elaboren y aprueben la ordenanza municipal o disposición de carácter general correspondiente.

En el supuesto en el que la gestión se lleve a cabo a través un contrato de gestión de servicio público, concretamente mediante la modalidad del concierto, al realizarse la gestión de la Escuela Infantil a través de una empresa privada o de un particular, el responsable de los ficheros no será la Administración, quedando por lo tanto los ficheros fuera del ámbito de aplicación de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, por tratarse de ficheros privados, y ajustándose para su creación a la regulación prevista en los artículos 25 y siguientes de la LOPD. Por lo tanto, la Administración no tendrá que declarar estos ficheros, al no ser la responsable de los mismos.

¿Puede la Real Escuela Superior de Arte Dramático crear un fichero de datos de carácter personal sobre currículos y publicar los datos obrantes en él en la página Web de la citada Real Escuela?

En primer lugar se deberá crear el fichero correspondiente, según el procedimiento previsto en el artículo 4 de la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid y desarrollado por el Decreto 99/2002, de 13 de junio.

Todas las personas cuyos datos personales sean incluidos en el fichero deberán ser informados del tratamiento que va a tener lugar en los términos que establece el artículo 5 de la LOPD.

En el formulario de recogida de datos que se utilice, deberá aparecer la siguiente cláusula, en la cual se de opción al alumno a marcarla o no, y de esta forma prestar su consentimiento para la publicación de los datos en la página Web: "Autorizo a que los datos de carácter personal facilitados a través de este formulario sean publicados en la página Web de la Real Escuela Superior de Arte Dramático con la finalidad exclusiva de que se conozca mi currículo para futuros trabajos".

¿Incluir en un fichero ya declarado de un Centro Educativo nuevos datos personales conlleva la creación de un nuevo fichero?

En principio, y haciendo una interpretación literal del artículo 4.2 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid y del artículo 7 del Decreto 99/2002, cualquier cambio en la descripción de la tipología de los datos declarados que figuren en la disposición de carácter general de creación del fichero y hayan sido declarados a la Agencia de Protección de Datos de la Comunidad de Madrid, implicará una modificación del fichero que necesariamente deberá aprobarse a través de una disposición de carácter general.

Sin embargo, si los nuevos datos que se pretenden recoger fueran adecuados desde un principio para la finalidad declarada del fichero (por ejemplo, incluir el dato de formación y titulación en un fichero cuya finalidad fuera expresamente la de "formación"), y encajaran en alguno de los apartados que fueron objeto de la declaración inicial del fichero, ello no debe implicar un cambio de la finalidad inicialmente declarada y en consecuencia no sería necesario realizar todo el procedimiento administrativo para la modificación de la declaración del fichero, siendo suficiente la notificación de dicho cambio a la Agencia, a través del apartado 7 del modelo aprobado por el Director de dicha Agencia.

¿En relación con la protección de datos de carácter personal, cuáles son las características principales del Registro de Historiales Académicos y de Alumnado Escolarizado en la Comunidad de Madrid? ¿Y del procedimiento telemático para su gestión?

La Agencia de Protección de Datos de la Comunidad de Madrid, de conformidad con lo dispuesto en el artículo 15.g) de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, ha emitido su informe en relación con el "Proyecto de Orden de la Consejería de Educación por la que se crea el Registro de Historiales Académicos y de Alumnado Escolarizado en la Comunidad de Madrid y se establecen los criterios generales y procedimientos telemáticos para su

gestión", remitido por la Secretaría General Técnica de la Consejería de Educación de la Comunidad de Madrid.

El Proyecto de Orden sometido a Informe, tiene por objeto regular "(…) la creación del Registro de Historiales Académicos y Alumnado escolarizado en la Comunidad de Madrid, de enseñanzas no universitarias, así como establecer los criterios generales de tramitación y los procedimientos telemáticos de gestión del Registro".

De acuerdo con lo dispuesto en su artículo 2.1, el Registro de cuya creación se trata extiende su ámbito de aplicación a los centros públicos y privados de la Comunidad de Madrid. En este aspecto, conviene señalar que el artículo 2 de la Ley 8/2001, atribuye a la APDCM competencia para ejercer funciones de control sobre los ficheros y tratamientos públicos de datos de carácter personal creados o gestionados por las Instituciones, Administraciones Públicas, Entes Locales, Universidades públicas y Corporaciones de derecho público, todas ellas de la Comunidad de Madrid.

En consecuencia, el contenido del informe que se emite, no entra a valorar consideraciones relativas a los procedimientos telemáticos de gestión en relación con el Registro de Historiales Académicos y Alumnados que se realicen en los centros privados de la Comunidad de Madrid, al resultar estos de competencia exclusiva de la Agencia Española de Protección de Datos.

Con carácter general, el apartado 2 del artículo 1 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, dispone que "Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias".

Entre otras "Finalidades" a las que se refiere la mencionada Ley, publicada en el BOE del 23 de junio de 2007, se establece que "Son fines de la presente Ley: (…) 3. Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos. 4. Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general. 5. Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones. 6. Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales. 7. Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general".

Por su parte, en el artículo 4 de dicha norma se prevén, entre otros "Principios generales" que:
"La utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose a los siguientes principios:

a) El respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la Ley Orgánica 15/1999, de Protección de los Datos de Carácter Personal, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.
(…)
d) Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".

En este contexto, la norma sometida a informe prevé la implantación telemática del Registro de Historiales Académicos y Alumnado escolarizados en la Comunidad de Madrid a través de procedimientos telemáticos integrados en el Sistema de Información de centros Educativos que la Comunidad de Madrid ya tiene implantados.
El citado Registro se inserta en el marco de las medidas que, en orden al impulso de la utilización de técnicas telemáticas por la Administración, se están desarrollando actualmente en el ámbito de la Comunidad de Madrid.

Quiere ello decir que una cuestión de esencial relevancia para la garantía del derecho fundamental a la protección de datos de carácter personal en la creación de este tipo de Registros informatizados, es la implantación de las adecuadas medidas de seguridad que garanticen la integridad y preserven la información de su acceso no autorizado.

Así, el artículo 3.3 del Proyecto de Orden, relativo a la utilización de procedimientos informáticos para el intercambio de información entre centros educativos, debe ponerse en conexión con lo dispuesto en la previsión general contemplada en el artículo 9 de la LOPD sobre las medidas de seguridad que deberán adoptarse en cualquier tratamiento de datos de carácter personal, a tenor de cuyo apartado primero, "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".

De acuerdo con el apartado segundo de dicho artículo "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".

En consecuencia, las condiciones, protocolos o criterios técnicos necesarios para el acceso a los datos deberán establecer las máximas garantías de seguridad, respetando siempre las exigencias contenidas en el citado precepto y, en particular en el Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que entró en vigor el 19 de abril de 2008.

Por este motivo, debería tenerse en cuenta la regulación contenida en las mencionadas disposiciones, a fin de asegurar el cumplimiento de las garantías del derecho fundamental a la protección de datos de carácter personal.

Por ello, se propone añadir un último inciso al artículo 3.3, siendo su redacción la siguiente: "El Registro de Historiales Académicos y Alumnado escolarizado en la Comunidad de Madrid desarrollará sus actuaciones utilizando procedimientos informáticos que favorezcan la integración e interoperabilidad entre sistemas de información, evitando duplicidades en la asignación de números de identificación y facilitando sistemas para el intercambio de información entre centros educativos, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo."

Respecto a la información a incorporar al "Registro de Historiales Académicos y Alumnado", el artículo 5 de la Orden hace referencia a la implantación de un sistema informático que gestione la información personal del alumno, según lo establecido en su Anexo I que recoge el contenido de la información básica que va a ser gestionada.
En atención al tratamiento de datos de carácter personal realizado por el Órgano administrativo consultante, debe recordarse que a los efectos previstos en la Ley Orgánica 15/1999, el "Registro de Historiales Académicos y Alumnado" deberá ser considerado como un fichero, conforme a la definición del artículo 3 b) del mismo, que señala que lo será "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

En consecuencia, tratándose de un fichero de Titularidad Pública, los datos de carácter personal recogidos en el citado Anexo deberán archivarse en ficheros previamente declarados por la Consejería de Educación, conforme a lo establecido en el Artículo 4 la Ley 8/2001, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.
En todo caso, también deberá tenerse en cuenta que el artículo 20.1 de la Ley Orgánica 15/1999 dispone que, "la creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente", siendo preciso que la disposición tenga el contenido mínimo previsto en el artículo 20.2.
Por este motivo, debe recordarse que, con posterioridad a la aprobación, en su caso, del Proyecto sometido a informe y antes de la efectiva puesta en marcha del Registro, será necesaria la aprobación de la norma de creación del fichero, que deberá incorporar los extremos exigidos por el artículo 20.2 de la Ley Orgánica 15/1999 y ser objeto de informe preceptivo de esta Agencia.
Dicho esto, respecto al consentimiento que deben prestar los interesados al tratamiento de sus datos de carácter personal, debe señalarse que, si bien el artículo 6.1 de la Ley Orgánica 15/1999, dispone que, "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.", el apartado 2º del propio artículo indica que dicho consentimiento no será preciso cuando los datos de carácter personal se refieran a las partes de un contrato o precontrato de una relación laboral y sean necesarios para su mantenimiento o cumplimiento.
Por tanto, en la medida en que los datos objeto del tratamiento sean únicamente los necesarios para el correcto desenvolvimiento de la relación negocial entre clientes y los datos sean necesarios para su mantenimiento y cumplimiento, no será necesario recabar el consentimiento del afectado. En caso contrario, será necesario requerir el consentimiento del interesado que deberá ser, conforme a lo dispuesto en el artículo 3 h), "libre, inequívoco, específico e informado", debiendo en consecuencia aparecer vinculado a las finalidades determinadas, específicas y legítimas que justifican el tratamiento de los datos, siendo así que los datos únicamente podrían ser tratados en

el ámbito de las mencionadas finalidades, tal y como dispone el citado artículo 4.1 de la Ley Orgánica, no pudiendo ser tratados para fines incompatibles con aquéllas (artículo 4.2 de la Ley Orgánica).
La manifestación de los requisitos legalmente exigidos al consentimiento del afectado se realiza en la práctica a través de la información al afectado, en el momento de la recogida de sus datos de carácter personal, de los extremos esenciales relacionados con el tratamiento, recabando a tal efecto su consentimiento en relación con los aspectos específica e inequívocamente hechos constar en la mencionada información.
El consentimiento, salvo cuando el tratamiento se refiera a los datos especialmente protegidos, regulados por el artículo 7 de la LOPD, podrá obtenerse de forma expresa o tácita, es decir, tanto como consecuencia de una afirmación específica del afectado en ese sentido, como mediante la falta de una manifestación contraria al tratamiento.
En todo caso, y aún el los supuestos de excepción a la prestación del consentimiento del interesado para el tratamiento de sus datos de carácter personal previstos en el artículo 6.2, la Ley impone el deber de información al afectado, al disponer su artículo 5.1 que "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".
En este sentido, y al objeto de cumplir con el deber de información, conforme al citado artículo 5.1 de la Ley, en aquellos modelos o solicitudes a través de los cuales se recaben datos de carácter personal deberá aparecer un texto informativo.
Para ello, y a modo de ejemplo, se deberá incluir en los modelos de solicitud de datos que, en su caso, se propongan, una cláusula como la siguiente:
"Los datos personales recogidos serán incorporados y tratados en el fichero "nombre del fichero", cuya finalidad es la adjudicación de las ayudas de libros de texto y material didáctico. Dicho fichero, está inscrito en el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org/apdcm) y el órgano responsable es "órgano responsable", con domicilio en …… donde el interesado podrá ejercer los derechos de acceso, rectificación o cancelación, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".
En el artículo 9 del Proyecto de Orden se hace referencia a la posibilidad de consulta de los datos que figuran en el Registro por parte de los centros y unidades de la Consejería que permita realizar gestiones que tienen encomendadas, añadiendo expresamente que, "Los centros docentes tendrán acceso a los registros generados por su solicitudes".
En relación con dichos acceso, deberá respetarse el "principio de calidad", consagrado en el ya citado artículo 4 de la Ley Orgánica 15/1999.
El artículo 4.1 de la Ley Orgánica 15/1999 dispone que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido", añadiendo el artículo 4.2 que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".

De este modo, cada centro docente únicamente estaría legitimado para acceder a los datos generados por ellos mismos, y siempre que el acceso se encuentre justificados.
Por este motivo, se propone la siguiente redacción para el apartado segundo del artículo 9: "Los centros docentes tendrán acceso a los registros generados por sus solicitudes, sin que sea posible el acceso a los datos por otros Centros".
En lo que se refiere a la indicación del centro directivo responsable del fichero y ante quién podrán ejercitarse los derechos de acceso, rectificación, cancelación y oposición que se mencionan en el artículo 10 apartado 2 y 4, se señala la conveniencia de identificar la dirección del responsable del tratamiento, a fin de garantizar el ejercicio por los interesados de sus derechos, indicándose asimismo, en caso de ser distinta de aquélla, la dirección en que será posible ese ejercicio.
Siguiendo con el contenido del artículo 10, el apartado 3 señala que "La unidad responsable del tratamiento de la información contenida en este fichero será Informática y Comunicaciones de la Comunidad de Madrid ICM".
En este sentido, considerando el artículo 9.2 de la Ley 8/2001 de Protección de Datos de Carácter Personal en la Comunidad de Madrid, cuando dispone que "Quienes presten servicios de tratamiento de datos de carácter personal a la Comunidad de Madrid y a las Entidades Locales en su ámbito territorial vendrán obligados a cumplir con lo previsto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre", debe señalarse que el papel de ICM (Informática y Comunicaciones de la Comunidad de Madrid), será el de encargado del tratamiento, definido en el artículo 3 g) de ambas leyes como "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".
Ello implicará el sometimiento de los citados laboratorios al régimen previsto en el artículo 12 de la Ley Orgánica 15/1999, caracterizado por las siguientes notas:
.- ?En lo que atañe a los requisitos formales, el artículo 12.2 impone que "la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".
.- ?Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece que "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".
.- ?En lo referente a la cesión de los datos, de lo establecido en el artículo 12.2 se desprende que no procederá esa cesión, de forma que los datos habrán de ser entregados única y exclusivamente al responsable del fichero. Se considera que será posible la subcontratación de estos servicios siempre y cuando se especifiquen los siguientes requisitos acumulativos, que deberán figurar en el contrato:
a) Que los servicios a subcontratar se hayan previsto expresamente en la oferta o en el contrato celebrado entre el responsable del fichero y el encargado del tratamiento.
b) Que el contenido concreto del servicio subcontratado y la empresa subcontratista conste en la oferta o en el contrato.
c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
.- ?En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.

.- ?Por último, según el artículo 12.4, "en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen."
Teniendo en cuenta la cuestión que acaba de señalarse, referida a la condición de encargado del tratamiento de ICM, podría resultar conveniente la inclusión de un precepto referido a este extremo. Así, el texto a añadir en el apartado que se analiza podría ser el siguiente:
"A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Informática y Comunicaciones de la Comunidad de Madrid, ICM tendrá la condición de encargada del tratamiento, debiendo respetar lo dispuesto en el artículo 12 de la misma."

Derechos de los ciudadanos

¿Tiene la APDCM datos de carácter personal de los alumnos y/o profesores? ¿Y de los ciudadanos en general?

No, la APDCM no tiene los datos de las personas incluidas en los ficheros inscritos en el Registro de Ficheros de Datos Personales. Únicamente dispone de la información relativa a la descripción de dichos ficheros, su finalidad, servicios o unidades ante los que se pueden ejercer los derechos de acceso, rectificación y cancelación, así como sobre los responsables de los mismos.

¿Cómo se puede dar cumplimiento al deber de información al interesado, que establece la LOPD, con carácter previo a la recogida de sus datos?

El Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, ha definido el derecho a la protección de datos como el derecho fundamental a la autodeterminación informativa, en virtud del cual, debe ser el interesado el que decida quién puede tener sus datos y para qué se usan. Para que este derecho sea efectivo es necesario que el ciudadano sea informado previamente, al objeto de que pueda ejercer su derecho de opción.
Para dar cumplimiento a este deber de información pueden utilizarse diferentes medios; el medio principal previsto por la LOPD es la inclusión de textos informativos en los impresos y cuestionarios que se utilicen. Una forma subsidiaria, que únicamente debe utilizarse en los supuestos en que resulte imposible la utilización de dichos impresos, formularios o cuestionarios, es la colocación de carteles informativos, accesibles a los alumnos y/o profesores, en los puntos en que se realice la recogida de los datos. En este último caso, deberá prestarse especial atención a que la información que figure en los carteles sea completa y detallada, y no genérica, y en particular contemplar todo lo especificado en el artículo 5 de la Ley Orgánica de Protección de Datos de Carácter Personal.
Debe analizarse en cada supuesto concreto, la forma de recogida de los datos, la naturaleza del colectivo del que se están recogiendo (menores, mayores, discapacitados, etc.) y la forma más efectiva para que se dé cumplimiento al deber establecido en la ley.

¿Cuándo cumplen con los términos del artículo 5 de la LOPD los impresos de los Centros Educativos utilizados para la recogida de datos de los alumnos? ¿Qué información ha de incluirse en los impresos por los que se solicita la concesión de la hipoteca joven de la Comunidad de Madrid?

Los impresos de recogida de datos de los alumnos deben contener en un pie de página una cláusula informativa en los términos del artículo 5 de la LOPD que, además, concuerde con lo establecido en el acuerdo de creación del fichero y que sea lo más completo posible porque sobre él se va a solicitar y obtener el consentimiento del alumno.
Con carácter general, siempre que se soliciten datos de carácter personal la LOPD obliga en su artículo 5 a que se cumpla con el derecho de información, es decir, previamente se ha de informar:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Igualmente señala dicho artículo que cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior, no siendo necesaria la información a que se refieren las letras b), c) y d) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
La APDCM viene recomendando la utilización del siguiente texto-tipo para el cumplimiento de las obligaciones derivadas del citado artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:
"Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla), y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es (indicarla), todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."
En el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid, parte de cuya información es accesible en línea a través de Internet en www.apdcm.es, figuran inscritos todos los ficheros declarados, entre los que se encuentran los ficheros creados por los centros educativos, de donde se podrán recoger todos los datos necesarios para personalizar el texto informativo del artículo 5.
En el caso de una solicitud de concesión de "hipoteca joven" de la Comunidad de Madrid existirán dos responsables de ficheros independientes: de un lado la Dirección de la Juventud de la Consejería de Educación y, de otro lado, una entidad bancaria. La actuación de la Agencia de Protección de Datos de la Comunidad de Madrid únicamente puede referirse al tratamiento realizado por la Consejería de Educación de la Comunidad de Madrid, pero no al tratamiento que efectúe el banco, dado que se trata de una empresa privada y el control del tratamiento de sus ficheros corresponde a la Agencia Española de Protección de Datos.

¿Cómo puede un alumno o un profesor conocer la información que de él mismo tiene su Centro Educativo? ¿Para ejercitar su derecho de acceso es suficiente que acompañe una copia de su DNI?

El derecho de acceso se ejerce mediante solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado, acompañando copia de su Documento Nacional de Identidad e indicando el fichero o ficheros a consultar.
Si bien es cierto que el derecho de acceso es un derecho personalísimo y debe ser ejercitado por el afectado (salvo las excepciones admitidas en la normativa correspondiente), también lo es que el afectado elige la forma en que desea ejercitar su derecho de acceso. Así, siguiendo lo establecido por el artículo 28 del Real Decreto 1720/2007, de 21 de diciembre:
"1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:
a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.

c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable".
La información proporcionada por el responsable del fichero deberá contener los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

¿Es posible denegar el ejercicio del derecho de acceso que la LOPD reconoce a los alumnos y/o profesores por la dificultad o el elevado coste que puede suponer su ejercicio?

No. La LOPD prevé que los datos de carácter personal sean almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

No obstante, la LOPD limita el ejercicio de ese derecho a los ciudadanos, pudiendo ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

¿Es conforme con la LOPD que un profesor cuyos datos están siendo objeto de tratamiento con motivo de su participación en un proceso selectivo que aún no ha concluido ejercite su derecho de acceso a los datos obrantes en un fichero sobre "Opositores Docentes"?

El artículo 15 de la LOPD regula el derecho de acceso en los siguientes términos:
"1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes."
Para enmarcar la cuestión, conviene señalar que el derecho de acceso que se menciona en la consulta, a efectos de la normativa sobre protección de datos de carácter personal, se refiere al derecho del afectado a obtener información sobre sus datos "sometidos a tratamiento".
El derecho de acceso constituye un derecho personalismo, de los reconocidos en la LOPD, derivado del derecho fundamental a la protección de datos reconocido como tal por la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, cuya tutela se atribuye a las Autoridades de Control en materia de protección de datos (Agencias de Protección de Datos), y cuyo ejercicio es gratuito.
En lo que se refiere al ejercicio de este derecho, el propio artículo 15.1 de la LOPD dispone que "el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos". En consecuencia, se establece -como regla general- un derecho de acceso

de los afectados de sus propios datos, sin quedar este sometido a ningún tipo de limitación.
Por otro lado, el hecho de facilitar al afectado sus propios datos de carácter personal tendría el carácter de un acceso efectuado por ellos mismos a la información que les concierne, encontrándose tal circunstancia perfectamente admitida por la Ley. Así, a mayor abundamiento, se otorga a los ciudadanos el derecho de acceso a los datos que les conciernan.
El desarrollo normativo de tal derecho se contiene en el artículo 27 de Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD que establece lo siguiente:
"1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.
2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.
No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.
3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común."
Por otra parte, la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, determina en su artículo 61 los sistemas selectivos de acceso a la función pública. En el caso de los funcionarios de carrera serán los de oposición y concurso-oposición, teniendo el sistema de concurso un carácter excepcional. En el supuesto del personal laboral fijo, los sistemas selectivos serán la oposición, el concurso-oposición y el concurso de valoración de méritos. De conformidad con el artículo 55 de la citada Ley, estos procedimientos de concurrencia competitiva se ajustan, entre otros, a los principios de publicidad de las convocatorias y de sus bases.
Los artículos 15 a 26, del Real Decreto 364/1995, de 10 de marzo, por el que se aprueba el Reglamento General de Ingreso del Personal al Servicio de la Administración General del Estado y de Provisión de Puestos de Trabajo y Promoción Profesional de los Funcionarios Civiles del Estado, aplicable a los procesos selectivos de la Administración de la Comunidad de Madrid, regulan los trámites administrativos de los procesos selectivos de acceso a la función pública, contemplando aquellos trámites y actos administrativos que serán objeto de publicación en el Boletín o Diario Oficial correspondiente.
Entre los trámites administrativos objeto de publicación con datos de carácter personal se encuentran los referentes a las listas de admitidos y excluidos, la relación de aprobados y el nombramiento como funcionarios de carrera.
En su Recomendación 2/2008, de 25 de abril, sobre Publicación de Datos Personales en Boletines y Diarios Oficales en Internet, en sitios Web institucionales y en otros medios electrónicos y telemáticos, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación en relación con estos procedimientos en los Boletines o Diarios Oficiales en Internet, se produzca únicamente en relación con los datos relativos al nombre, apellidos, número del Documento Nacional de Identidad, puntuación total obtenida y nombramiento como funcionarios de carrera de las personas que obtuvieron las plazas. Asimismo, se recomienda la aplicación de dicha norma cuando se trate de procesos de acceso a la

Administración pública que afecten a personal laboral. Especialmente, se recomienda que, en ningún caso, se proceda a la publicación en el Boletín o Diario Oficial en Internet de los datos de carácter personal de aquellos aspirantes que no hayan superado dicho proceso.
A su vez, en relación con la publicación de la relación definitiva de aprobados, en la mencionada Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, se señala que debe tenerse en cuenta que la minusvalía es un dato de salud, por lo que se recomienda que la publicación de dicha relación contenga la información mínima relativa al hecho de la discapacidad, sin incluir referencia alguna al grado o el tipo de la misma.
Por lo que respecta al contenido concreto de la pregunta, la APDCM recomienda que el acceso a los actos de trámite que contengan datos de carácter personal en los procesos selectivos, y, en especial, los referentes a las calificaciones obtenidas por los aspirantes en los distintos exámenes y pruebas realizadas, las adaptaciones concedidas a dichos aspirantes que concurran por el turno de discapacidad y la convocatoria de los aspirantes para realizar los exámenes o proceder a la lectura de los mismos, se realice únicamente mediante el acceso identificado y restringido a los interesados, exigiéndose la acreditación indubitada de su identidad, tanto en el supuesto de que dicho acceso se realice al expediente administrativo en "formato papel", como cuando el mismo se realice a través de un sitio Web institucional, en un canal electrónico o telemático de la Administración u Órgano administrativo convocante, o a través de un tablón de anuncios (tradicional o electrónico) del Órgano competente.
En cualquier caso, deberá garantizarse que únicamente los interesados en el procedimiento selectivo puedan acceder a los datos personales de terceras personas relacionados con dicho procedimiento, exigiéndose -como requisito indispensable- que la identificación y autenticación del ciudadano que realice dicho acceso se realice mediante la presentación de la documentación que identifique al interesado, o bien a través del uso de sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios, como la introducción de una clave de acceso personalizada previamente asignada por la Administración, con su correspondiente contraseña, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
A su vez, sin perjuicio de todo lo anterior, se podrá proceder a la publicación de los citados trámites en el sitio Web de la Administración u Órgano administrativo convocante, sin la exigencia de un sistema de acceso identificado o restringido, en aquellos supuestos en que se solicite con carácter previo el consentimiento para dicha publicación a los aspirantes. A dichos efectos se considera que este consentimiento debe ser diferente del consentimiento que presta el aspirante para participar en el proceso selectivo. Para la solicitud de dicho consentimiento se estima como medio idóneo para la obtención del mismo su solicitud a través del modelo utilizado por el ciudadano afectado para participar en el proceso selectivo correspondiente.
En estos supuestos, se recomienda que en la Orden o Resolución que convoque el procedimiento de acceso a la función pública o de ingreso como empleado público, se contemple dicha forma de publicación de los distintos actos de trámite.
Por otro lado, conviene insistir en que el derecho de acceso al que estamos haciendo referencia resulta independiente del que puedan otorgar a los ciudadanos las leyes especiales y en particular la Ley 30 /1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.
Es por este motivo que la cuestión podría plantearse desde el ejercicio del derecho de acceso a la documentación obrante en el procedimiento de aquellos que tengan la consideración de interesado, por aplicación de los principios establecidos en la mencionada Ley 30/1992, de 26 de noviembre.

En estos términos, dicha norma, con carácter general, respecto del acceso a archivos y registros, establece en su artículo 37 que:
"1. Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud."
En las actuaciones objeto de la presente pregunta, hay que señalar que el procedimiento no se encuentra concluido en la fecha de la misma, por lo que el apartado 37.1 no sería de aplicación a dicho supuesto.
En cuanto a la posible condición del interesado solicitante del acceso, el artículo 31 de la Ley 30/1992, de 26 de noviembre, delimita jurídicamente el concepto de interesado en el procedimiento administrativo, indicando a tal efecto que se considerarán como tales en el procedimiento:
"a) Quienes lo promuevan como titulares de derechos o intereses legítimos individuales o colectivos; b) Los que, sin haber iniciado el procedimiento, tengan derechos que puedan resultar afectados por la decisión que en el mismo se adopte; y c) Aquellos cuyos intereses legítimos, individuales o colectivos, puedan resultar afectados por la resolución y se personen en el procedimiento en tanto no haya recaído resolución definitiva".
A su vez, el artículo 35.a) de la misma Ley recoge el derecho de los ciudadanos "A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos".
Ello no obstante, sería posible entender que de este derecho debe excluirse el derecho a la obtención de copias de documentos respecto de los que el artículo 37 de la Ley 30/1992, de 26 de noviembre, impide su consulta, entre los que se incluyen aquellos que contengan datos "referentes a la intimidad de las personas".
Así, el mencionado artículo 37 de la Ley 30/1992, de 26 de noviembre, regula el derecho de los ciudadanos a los archivos y registros públicos, especificando que:
"2. El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno.
3. El acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas figuren en los procedimientos de aplicación del Derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo.
4. El ejercicio de los derechos que establecen los apartados anteriores podrá ser denegado cuando prevalezcan razones de interés público, por intereses de terceros más dignos de protección o cuando así lo disponga una ley, debiendo, en estos casos, el órgano competente dictar resolución motivada."
En atención a lo anterior, el Órgano consultante deberá estar a lo dispuesto en la normativa indicada, relativa a la regulación sobre del derecho de acceso a archivos y registros contenida en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, no resultando directamente aplicable las previsiones contenidas en la LOPD. En consecuencia, será el órgano que deba decidir sobre la petición al que corresponda resolver -de manera motivada- sobre la procedencia de entregar o no la

documentación que se solicita en función de lo previsto para este tipo de supuestos por el artículo 37 de la citada Ley 30/1992, de 26 de noviembre.

¿Vulnera la LOPD el hecho de tomar fotografías de alumnos en centros escolares?

De acuerdo con el tenor literal del artículo 2 de la LOPD, dicha Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Por tanto, para que el hecho descrito en la pregunta se encuentre dentro del ámbito de aplicación de la LOPD es necesario que las fotografías tomadas sean registradas en un soporte físico que permita su tratamiento; es decir, que exista un fichero. Sin embargo, de los antecedentes remitidos no puede deducirse si existe tal fichero. En caso de que así fuera, lo más probable, dada la descripción de los hechos y al ser la madre de una alumna del centro quien toma las fotografías, es que se tratara de un fichero de carácter doméstico. Este tipo de ficheros están excluidos del ámbito de aplicación de la LOPD al amparo del artículo 2.2 a) de dicha norma.
En efecto, de acuerdo con lo dispuesto por el artículo 2.2 a) de la LOPD, el régimen de protección de los datos de carácter personal que se establece en la dicha Ley Orgánica no es de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
A su vez, se señala que, dada la escasa probabilidad de que, según los antecedentes remitidos, exista una vulneración de la LOPD, es necesario considerar si es posible que los hechos descritos constituyan una vulneración del derecho a la propia imagen de los alumnos y profesores.
Dicho derecho se encuentra regulado en el artículo 18 de la Constitución Española y desarrollado por la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen. Son titulares de dicho derecho todas las personas, incluidos, por tanto, los menores de edad, quienes podrán prestar su consentimiento por si mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil, o por escrito de sus representantes legales (artículo 3 de la LO 1/1982).
Según el artículo 7 de dicha Ley Orgánica, tendrá la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo 2 de esta Ley (…): 5. La captación, reproducción o publicación por fotografía, filme, o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2.
Por tanto, en términos abstractos, la captación de la imagen de los alumnos y profesores sin su consentimiento sí que puede constituir una vulneración del derecho regulado en la Ley Orgánica 1/1982. Sin embargo, existe una importante limitación al derecho a la propia imagen, los usos sociales, que obliga a atender a los aspectos concretos del hecho comunicado a la APDCM y las circunstancias. Así, dispone el artículo 2 de la Ley Orgánica 1/1982 que "La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia".
De esta manera, habrá que tener en cuenta en qué medida la captación de imágenes de alumnos y profesores por parte de la madre de una alumna excede de lo que se tiene por costumbre, ya que es habitual que los padres de alumnos tomen fotografías como recuerdo de sus hijos y compañeros en el colegio. En todo caso, corresponde a los órganos jurisdiccionales, a través de los procedimientos enunciados en el artículo 9

de la Ley Orgánica 1/1982, determinar si ha habido vulneración del derecho a la propia imagen.
En atención a todo lo anterior, en nuestra opinión, habrá de estarse a lo dispuesto en la citada Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen, correspondiendo, en su caso, a los órganos jurisdiccionales competentes sobre dicha materia la determinación de si se ha producido la vulneración del derecho a la propia imagen de las personas fotografiadas.
En conclusión, la LOPD será de aplicación únicamente si las fotografías se registran en un fichero que permita su tratamiento, y siempre que el fichero no sea de carácter doméstico. En su caso, la posible vulneración del derecho a la propia imagen de alumnos y profesores por parte de los padres, deberá analizarse a la vista de lo regulado en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen, correspondiendo la decisión al respecto a los órganos jurisdiccionales.

Calidad de datos.

¿Qué datos pueden recogerse de los alumnos y/o de los profesores para el ejercicio de una determinada actividad por parte de un Centro Educativo?

De acuerdo con el principio de calidad de los datos que establece la LOPD, sólo podrán recogerse, así como someterse a tratamiento, aquellos datos que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
El principio de calidad debe interpretarse no como limitativo en cuanto al número y tipo de datos que puedan utilizarse, sino como promotor de un criterio de racionalidad en el manejo de la información.

¿Los datos recogidos para una determinada finalidad pueden utilizarse para cualquier otra que se pueda plantear a posteriori?

Los datos sólo se pueden recabar para cumplir una finalidad determinada, explícita y legítima, que además deberá conocer el interesado, como regla general, con carácter previo a la recogida de sus datos.
Los datos no podrán utilizarse para finalidades incompatibles con aquellas para las que hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos, aunque la recomendación normal es que estas tareas se realicen con datos disociados, eliminando cualquier dato que identifique o permita identificar a las personas.
Por ejemplo, es legítimo recabar los datos de los alumnos matriculados en el último curso del primer ciclo educativo para llevar a cabo un estudio cuya finalidad sea adecuar los servicios de formación profesional a las expectativas de dichos alumnos, pero los datos así recogidos no podrán utilizarse, por ejemplo, para realizar una campaña publicitaria entre esos alumnos por parte de un centro privado que se dedique a impartir enseñanza.

¿Puede cualquier empleado de un centro público de enseñanza acceder a los datos de carácter personal contenidos en los ficheros?

No todas las personas que constituyen una organización deben acceder a todos los datos personales. Dentro de la finalidad a la que se refiera el fichero, cada empleado sólo deberá tener acceso a aquéllos datos que resulten necesarios para el cumplimiento de sus funciones, cumpliendo así con el principio de calidad de los datos.

En consecuencia, únicamente accederán a aquéllos datos personales que resulten adecuados, pertinentes y no excesivos para el cumplimiento de sus funciones.

¿Puede utilizarse el dato del teléfono móvil de los alumnos, de los padres o de los profesores para la remisión de mensajes de texto vía SMS?

Para que se pueda enviar al teléfono móvil que faciliten los alumnos, los padres o los profesores, mensajes SMS sobre temas relacionados con la actividad del centro educativo, en primer lugar debe incluirse expresamente el dato del teléfono móvil en el formulario correspondiente y, en segundo término, debe informarse al interesado del uso del dato del teléfono móvil para esta finalidad, dado que los mismos se pueden oponer a este tratamiento.

Cesiones de datos de los alumnos de los Centros Educativos
¿Las calificaciones académicas de los alumnos de un Centro Educativo pueden publicarse en los tablones o en Internet?

Los expedientes académicos de los alumnos no constituyen un procedimiento de concurrencia competitiva que justifique la publicación de las calificaciones (no existe una disposición de carácter general de la Consejería de Educación que apruebe la convocatoria previa del número total de aprobados de cada curso académico). El número de aprobados y de suspensos lo determinará cada profesor, en función de los conocimientos adquiridos y de la realización de los exámenes o pruebas que haya superado o no cada alumno.
No hay que confundir la publicación de estas calificaciones con la posibilidad de publicar los listados de aspirantes con sus resultados de un proceso selectivo tales como las pruebas de acceso a la Universidad, los premios extraordinarios de carrera, contratación de personal, etcétera. En estos casos será posible la publicación siempre y cuando la convocatoria determine expresamente el lugar de publicación (tablones de anuncios, páginas Web, etc.) y ello porque en estos supuestos rige el principio de publicidad y así viene previsto específicamente en el artículo 59.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
Con carácter general, las notas de calificación de cada asignatura tienen como destinatario al alumno, anotándose en su expediente académico. En consecuencia la difusión de dichas notas de calificación a través de los tablones de anuncios del centro educativo o a través de Internet, constituye una cesión de datos de carácter personal de los alumnos. Así, en principio, para que pueda realizarse una cesión de datos personales debe existir consentimiento de los interesados o bien, entre otras excepciones establecidas por la LOPD, deberá existir una norma con rango de Ley que exima de dicho consentimiento.
Únicamente en el supuesto de los alumnos universitarios, la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, establece en su apartado tercero que "No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación".
En lo referente a la publicación de calificaciones en el resto de ámbitos educativos, la Ley Orgánica 2/2006, de 3 de mayo, de Educación, no contiene ninguna referencia específica que habilite la publicidad de dichas calificaciones obtenidas por los estudiantes a través de tablones de anuncios o de sitios Web institucionales.
No obstante lo anterior, la Agencia de Protección de Datos de la Comunidad de Madrid, entiende que, en muchas ocasiones, esta publicación puede estar justificada en virtud de los principios de mérito y capacidad que rigen en materia de Educación, siempre que no se afecte al libre desarrollo de la personalidad de los individuos afectados.
En este sentido, no debe olvidarse que todos los ciudadanos tienen derecho a acceder a la educación en función de sus aptitudes y vocación, sin que en ningún caso el ejercicio de este derecho esté sujeto a discriminación, debiendo prevalecer el principio de igualdad y los valores de mérito y capacidad. Dichos derechos deben garantizarse por las Administraciones públicas y Órganos administrativos competentes de acuerdo con el principio de objetividad, tal y como se reitera en la Recomendación 2/2008, de 25 de abril, de la APDCM.

De este modo, en el supuesto de publicación de calificaciones de los estudiantes no universitarios a través de un sitio Web institucional, de canales electrónicos o telemáticos, o de tablones de anuncios (tradicionales o electrónicos), deberá garantizarse el acceso restringido de dichos estudiantes, o de la persona que ostente su patria potestad o tutela, a sus propios datos personales, facilitando dicho acceso mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios como el uso de un nombre de usuario y una contraseña segura, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.

En consecuencia, se recomienda que no se proceda a publicar en Internet, a través de sitios Web institucionales, canales electrónicos o telemáticos, ni tablón de anuncios (tradicionales o electrónicos) que posibiliten el acceso no identificado, las calificaciones de los alumnos de educación infantil, educación secundaria obligatoria, bachillerato, formación profesional, enseñanzas de idiomas, enseñanzas artísticas, enseñanzas deportivas, educación para personas adultas y pruebas de acceso a la universidad (para mayores de 25 años y de selectividad), salvo que se obtenga el consentimiento previo y expreso de los alumnos afectados.

En todo caso se recomienda que cuando las calificaciones se publiquen en el sitio Web institucional, en canales electrónicos o telemáticos, o en tablones de anuncios (tradicionales o electrónicos), de conformidad con el principio de finalidad establecido en el artículo 4 de la LOPD, una vez transcurrido el plazo establecido para presentar posibles reclamaciones y/o alegaciones en relación con dichas calificaciones por parte los alumnos o por la persona que ostente su patria potestad o tutela, dichos datos de carácter personal sean objeto de cancelación, supresión o borrado del sitio Web, del canal o del tablón de anuncios correspondiente.

A su vez, por parte del responsable de fichero deberá tenerse en cuenta que el propio artículo 4 de la LOPD (principio de calidad de los datos) establece que los datos personales sólo podrán ser sometidos a tratamiento (lo que incluiría su cesión a terceros a través de la publicación) "cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

¿Cuáles son las fórmulas legales de publicación de los resultados de los siguientes procesos: Prueba de Acceso a estudios universitarios (Selectividad), Prueba de Acceso a la Universidad de los Mayores de 25 años y Proceso de Ingreso?

Las convocatorias de este tipo de procedimientos constituyen un claro ejemplo de procedimientos selectivos en régimen de concurrencia competitiva, sujetos al principio de publicidad, siéndoles de aplicación lo dispuesto en el artículo 59 de la Ley 30/1992, de 26 de noviembre (LRJPAC). En dicho artículo se establecen las normas para notificar los actos administrativos, estableciendo en su apartado 5 que la publicación del acto sustituirá a la notificación en el caso de que se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.

Tanto las pruebas de acceso a la Universidad para mayores de 25 años, como el procedimiento para las pruebas de acceso a estudios universitarios, son procedimientos administrativos de concurrencia competitiva y están sujetos al principio de publicidad. Para cumplir con el derecho de información del artículo 5 de la LOPD, se recomienda incluir en los formularios de solicitud la siguiente cláusula:

"Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla), y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación,

cancelación y oposición ante el mismo es (indicarla), todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."

¿Es posible publicar en la página Web los datos que figuran en el acta de calificación de la convocatoria de los premios extraordinarios de bachillerato que otorga anualmente la Comunidad de Madrid?

La concesión de los premios extraordinarios de bachillerato es un procedimiento administrativo de concurrencia competitiva, que se tramita de conformidad con la convocatoria aprobada por la Consejería de Educación de la Comunidad de Madrid, y está sujeto al principio de publicidad, siéndole de aplicación lo dispuesto en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En dicho artículo se establecen las normas para notificar los actos administrativos, estableciendo en su apartado 5 que la publicación del acto sustituirá a la notificación en el caso de que se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.

En este sentido, cabe citar el artículo 1.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, cuando dispone que las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en dicha Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

A su vez, en el artículo 4 de dicha norma se prevé que la utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose, entre otros principios, al respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la LOPD, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.

La publicación de los resultados obtenidos por los alumnos tiene la finalidad de hacer efectiva la práctica de la notificación del acto administrativo, que en este caso es el acta de calificación, y posibilitar que se puedan formalizar las oportunas reclamaciones contra dicho resultado ante el Tribunal. Dicha publicación en las correspondientes páginas Web daría cumplimiento a lo señalado en el 1.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, respetando en todo caso el principio de calidad de los datos, establecido en el artículo 4 de la LOPD según el cual, los datos deberán ser adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explicitas y legitimas para las que se hayan obtenido.

No obstante se debe incluir en el impreso de solicitud de participación en la convocatoria la siguiente leyenda informativa:

"Los datos personales recogidos, serán tratados con su consentimiento informado en los términos del artículo 5 de la Ley Orgánica 15/1999, y de conformidad a los principios dispuestos en la misma y en la ley 8/2001 de la Comunidad de Madrid, pudiendo ejercer el derecho de acceso, rectificación, cancelación y oposición ante el responsable del fichero".

Asimismo, a la hora de publicar los listados de calificaciones en la página Web se incluirá el siguiente texto:

"Los listados que se publican en esta página Web y que contienen datos de carácter personal se ajustan a la legislación actual de protección de datos y su única finalidad, de conformidad con lo previsto en el artículo 59 de la Ley 30/1992, de 26 de noviembre,

de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, es la de proceder a notificar a cada uno de los aspirantes el contenido del procedimiento selectivo. Estos listados no constituyen fuente de acceso público y no podrán ser reproducidos ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados."

¿Puede un profesor acceder al expediente académico de un alumno?

En la medida en que un profesor tiene una relación directa con cada uno de sus alumnos tendrá legitimidad para acceder a los expedientes académicos de cada uno de ellos, siempre que dicho acceso tenga una finalidad académica y por tanto compatible con las finalidades declaradas del fichero. Sin embargo, hay que señalar que el acceso de los profesores al Fichero Expedientes de Alumnos o Gestión Académica no debería ser indiscriminado, sino que cada profesor debería tener acceso solamente a los datos de sus propios alumnos, pues no estaría justificada la finalidad del acceso a los datos del resto de los alumnos.
En consecuencia, el responsable del fichero deberá establecer los controles de acceso necesarios para cumplir con esta medida, teniendo en consideración lo previsto en el artículo 91 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

¿Puede repartirse entre los miembros del Consejo Escolar las notas de todos los alumnos con sus nombres para analizar sus dificultades específicas e impulsar las mejoras necesarias?

Repartir entre los miembros del Consejo Escolar las calificaciones de todos los alumnos con sus nombres para analizar las dificultades que puedan tener e impulsar las mejoras necesarias, podría ser contrario al artículo 4 de la LOPD. Se trataría de un acceso excesivo a la información de carácter personal que no se encontraría justificado pues, de acuerdo con la propia pregunta, el total de los alumnos no necesitara mejorar, ni tendría dificultades de aprendizaje; únicamente un número determinado de ellos precisaría de atención específica. En consecuencia, sería únicamente respecto de estos alumnos sobre los que habría que interactuar.
Por tanto, la APDCM considera que es más adecuado para el fin que se persigue que, con carácter previo, en el claustro de profesores, que es el órgano del centro escolar que evalúa a cada alumno, se determine cuales son los alumnos que pueden tener dificultades y precisen ayuda, siendo sobre estos alumnos sobre los que el Consejo Escolar pueda tener acceso a sus calificaciones.
No obstante, también seria factible que se comunicasen al Consejo Escolar, de forma disociada, las calificaciones de los alumnos de tal forma que la información no se pudiese asociar con personas identificadas o identificables.

¿Los padres y tutores de los alumnos tienen derecho a solicitar las calificaciones académicas del Centro Educativo?

Como regla general, si los alumnos son menores de edad, los padres y tutores tienen derecho a solicitar del centro educativo las calificaciones académicas de sus hijos. Por el contrario, en el caso de que los alumnos sean mayores de edad no se podrán ceder, ya que constituiría una comunicación de datos personales no amparada por las excepciones que contempla la ley.
En concreto, en relación a los menores de edad, se plantea si en la cesión de sus datos académicos a sus padres o tutores sin su consentimiento, debe prevalecer la

voluntad de un alumno menor de edad que no quiera que se faciliten sus calificaciones académicas a sus padres o tutores sobre la pretensión de éstos de acceder a dicha información, no pudiendo en dicho caso el centro educativo atender dicha solicitud de los padres o tutores.
En cuanto a la posibilidad de ceder los datos académicos de los menores a sus padres o tutores sin el consentimiento de dichos menores afectados, ante todo, deberá considerarse que la comunicación de los datos al padre, madre, tutor o representante legal, supone una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley como "Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado."
Respecto de las cesiones, el artículo 11.1 prevé taxativamente que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado." Este consentimiento sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2 de la Ley, entre los que se encuentra la posibilidad de que una norma con rango de Ley habilite la cesión.
En este supuesto, de acuerdo con lo dispuesto por el artículo 154 del vigente Código Civil, los hijos no emancipados están bajo la potestad del padre y de la madre. La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y comprende los siguientes deberes y facultades:
1.- Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.
2.- Representarlos y administrar sus bienes (.....).
En consecuencia, en principio, dado que la facultad de acceder a la información de carácter académico (entre la que se cita la cesión relativa a las calificaciones obtenidas por los menores en el centro educativo), se encuentra dentro del marco de los deberes y derechos que corresponden a los padres, inherentes al ejercicio de su patria potestad, cabría concluir que en el supuesto de los hijos no emancipados existe una norma legal habilitante que ampara la cesión de los datos académicos de los menores a sus padres, derivada de lo previsto en el artículo 154 del Código Civil.
En lo que a los tutores se refiere, podría argumentarse que idéntica previsión, constitutiva de la habilitación legal exigida por el artículo 11.2 a) de la LOPD, se encuentra en lo dispuesto por el artículo 269 del citado Código Civil, cuando dispone que el tutor está obligado a velar por el tutelado y, en particular:
1. A procurarle alimentos.
2. A educar al menor y procurarle una formación integral.
3. A promover la adquisición o recuperación de la capacidad del tutelado y su mejor inserción en la sociedad.
4. A informar al Juez anualmente sobre la situación del menor o incapacitado y rendirle cuenta anual de su administración.
En consonancia con dicho precepto, para los tutores, inicialmente, podrían obtenerse similares conclusiones que las expuestas más arriba para los padres que ejercen la patria potestad, por lo que la cesión de los datos personales relativos a las calificaciones académicas de los menores resultaría conforme con lo previsto por la LOPD.
Sin embargo, existen argumentos jurídicos que apuntan claramente en orden a la fijación de determinados límites a la patria potestad -también en materia educativa- de los padres y madres, así como a las facultades de los tutores legales, en el supuesto de los menores de edad que hayan cumplido los dieciséis años.
Así, por una parte, el artículo 13.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, ha establecido que "podrá procederse al tratamiento de los datos de los mayores de catorce años con su

consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores".
En consecuencia, esta regla de los catorce años no se aplica "en aquellos casos en los que la Ley exija para la prestación del consentimiento la asistencia de los titulares de la patria potestad o tutela" -art. 13.1 del Reglamento-, lo que ocurre especialmente en el ámbito educativo, sobre todo en aquellos supuestos donde están siendo objeto de tratamiento datos especialmente protegidos.
A su vez, el hecho de que el menor consienta al tratamiento de datos personales o acceda a la información personal no significa que no puedan acceder sus padres o las personas que ostentan su representación legal. Existe aquí una importante contradicción entre el derecho a la protección de datos personales de los menores -que implica la oposición al acceso por parte de terceras personas- y el ejercicio de la patria potestad y de la representación legal que implica el acceso a la información personal.
Este delicado equilibrio debe inclinarse a oponerse al acceso de los padres o de los representantes legales para proteger la libertad y el libre desarrollo de la personalidad cuando el menor tenga ya dieciséis años, salvo que se trate de un tema grave o de una cuestión de trascendental importancia para el menor, permitiendo únicamente el acceso a los datos de los mayores de dieciséis años en los supuestos imprescindibles para el ejercicio de la patria potestad. En cambio, hasta la edad de dieciséis años prevalece las funciones que conllevan el ejercicio de la patria potestad en el ámbito educativo, derivadas de lo dispuesto en los artículos 154 y 269 del Código Civil.
Por otra parte, abonando esta tesis -mantenida por la Agencia de Protección de Datos de la Comunidad de Madrid-, existen importantes normas sectoriales específicas. Así, la Ley de la Comunidad de Madrid 5/2002, de 27 de junio, de Drogodependencia, señala que "en el caso de que un menor de dieciséis años precise atención sanitaria por consumo de bebidas alcohólicas u otras drogas, los centros o servicios sanitarios que presten atención, deberán comunicar la situación del menor a los padres o tutores para que éstos se hagan cargo del menor. Asimismo, también se pondrá en conocimiento de dichos padres o tutores cuando fuese menor de dieciocho años y la situación, a juicio del facultativo, pudiera considerarse de gravedad". Este precepto establece la misma franja de edad que el art. 9.3 c) de la Ley 41/2002, de 14 de noviembre, de "autonomía del paciente", que establece la obligación de informar a los padres de menores emancipados o con dieciséis años cumplidos "en caso de actuación de grave riesgo, según el criterio del facultativo".
Específicamente en materia educativa, el artículo 4 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, dispone que "1. La enseñanza básica a la que se refiere el artículo 3.3 de esta Ley es obligatoria y gratuita para todas las personas. 2. La enseñanza básica comprende diez años de escolaridad y se desarrolla, de forma regular, entre los seis y los dieciséis años de edad". Por su parte, en el artículo 22 de dicha Ley Orgánica se establece que "La etapa de educación secundaria obligatoria comprende cuatro cursos, que se seguirán ordinariamente entre los doce y los dieciséis años de edad".
Dichos preceptos deben ponerse en relación con lo previsto en la legislación sobre protección del menor, contenida en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, en cuyo artículo 2 (Principios generales) se establece que "En la aplicación de la presente Ley primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir. Asimismo, cuantas medidas se adopten al amparo de la presente Ley deberán tener un carácter educativo. Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva".

En conclusión, a juicio de la APDCM no resultaría conforme con la LOPD el acceso de los padres a las calificaciones de los hijos mayores de dieciséis años sin su consentimiento, no debiendo acceder -sin el consentimiento de los menores, mayores de dieciséis años- a las calificaciones de los mismos.
En segundo lugar, se plantea si, dado que existe una relación jurídica entre el centro educativo y los padres que no puede ser asumida por el menor, sería lícito facilitar dichas calificaciones como resultado de los servicios prestados. Además, se cuestiona si en el caso de que el alumno tuviera problemas de adaptación en el centro educativo, el hecho de comunicarlo a sus padres podría ser constitutivo de infracción, conllevando la correspondiente sanción, de acuerdo con lo dispuesto en la LOPD. Igualmente, se plantea idéntica cuestión en el supuesto de que los datos sean solicitados por los servicios sociales de una Comunidad Autónoma que actúe como tutor del menor.
En relación con estas cuestiones, debe señalarse que no resulta aplicable lo previsto por el artículo 11.2 c) de la Ley Orgánica 15/1999, cuando dispone que "el consentimiento exigido en el apartado anterior no será preciso (...) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros (…)", debiendo considerarse idéntica argumentación que la expuesta en los párrafos anteriores.
En consecuencia, con independencia de la existencia de una relación jurídica entre el centro educativo y los padres o tutores del menor, la cesión de los datos relativos a las calificaciones académicas de éste, así como la comunicación de cualquier circunstancia relativa a la adaptación o inadaptación del menor en el centro educativo, se encontrará amparada legalmente, con carácter general y con las excepciones a las que se ha hecho mención (mayores de dieciséis años), por los artículos 154 y 269 del vigente Código Civil.
Igualmente, en el supuesto de que los datos sean solicitados por los servicios sociales de la Comunidad de Madrid que actúen como tutor del menor, resultará aplicable la habilitación legal contenida en el artículo 269 del citado Código Civil (también con excepción del acceso a las calificaciones académicas de los mayores de dieciséis años), sin perjuicio de la existencia de otras normas de ámbito estatal y autonómico que ofrezcan idéntica cobertura en atención a las funciones legalmente conferidas a dicha Comunidad Autónoma cuando actúe en su condición de tutor del menor.
¿En qué casos procede la cesión de datos personales a la policía por parte de los Centros Educativos?
Según establece el artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. Sin embargo, no será preciso dicho consentimiento para recoger datos de carácter personal si así viene establecido en una ley, o cuando se recojan en el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
Asimismo, la LOPD establece en el artículo 11.1 la norma general del consentimiento expreso del afectado para llevar a cabo una comunicación de datos de carácter personal. Sin embargo, dicha regla general no es absoluta, y así, el propio artículo 11 regula en su apartado 2 una serie de excepciones a la misma. Entre dichas excepciones se encuentran las siguientes: la posibilidad de que una ley regule expresamente la cesión; que los datos procedan de una fuente de acceso público; la existencia de una relación jurídica cuyo desarrollo y control implique necesariamente la conexión con ficheros de terceros; cuando el destinatario de la cesión sea el Defensor del Pueblo, el Ministerio Fiscal o los jueces y Tribunales; cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior con fines estadísticos, científicos o históricos.

Atendiendo a la normativa específica, el artículo 4 de la Ley Orgánica 2/1986, de 13 de marzo, Reguladora de las Fuerzas y Cuerpos de Seguridad, establece que todos tienen el deber de prestar a las Fuerzas y Cuerpos de Seguridad el auxilio necesario en la investigación y persecución de los delitos en los términos previstos legalmente.
En el artículo 5 se enumeran los principios básicos de actuación de los miembros de las Fuerzas y Cuerpos de Seguridad, encontrándose entre éstos el ejercicio de su función con absoluto respeto a la Constitución y al resto del ordenamiento jurídico, así como guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones, no estando obligados a revelar las fuentes de información salvo que el ejercicio de sus funciones o las disposiciones de la Ley les impongan actuar de otra manera.
Los ficheros policiales poseen una regulación especial contenida en el artículo 22 de la LOPD y, con base en ella, la recogida y tratamiento para fines policiales de datos de carácter personal de los centros educativos, por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
Este artículo habilita a las Fuerzas y Cuerpos de Seguridad para la obtención y tratamiento de los datos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan las siguientes condiciones:
o Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales. La obtención de los datos por parte de la Policía deberá basarse en dichas razones y, tratándose de datos especialmente protegidos, los datos deberán resultar absolutamente necesarios para los fines de una investigación concreta. En todo caso la cesión quedará limitada al uso derivado de la función de mantenimiento de la seguridad pública.
o Que se trate de una petición concreta y específica, al no ser compatible con lo señalado las solicitudes masivas de datos. La petición se limitará a datos personales concretos, debidamente individualizados, solicitados por las Fuerzas y Cuerpos de seguridad en el marco de las competencias que tengan atribuidas por la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
o Que la petición se efectúe con la debida motivación, que acredite su relación con lo supuestos que se han expuesto, dejando constancia de la petición. La petición policial, debidamente motivada, se dirigirá al Responsable del tratamiento, acreditándose la existencia de una investigación policial en curso. La solicitud deberá cursarse a través de un soporte documental que permita dejar constancia de la misma, resultando admisible a dichos efectos la expedición de un oficio u orden de servicio extendidos por parte de la propia Policía encargada de las actuaciones.
o Que los datos sean cancelados cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento, en cumplimiento del artículo 22.4 de la LOPD. Corresponderá a las Fuerzas y Cuerpos de Seguridad cesionarios garantizar la confidencialidad y seguridad de los datos personales cedidos.
Por lo que se refiere a las funciones que deberán ejercer los Cuerpos de policía local, el artículo 53 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad establece -específicamente- en su apartado 1: "e) Participar en las funciones de policía judicial, en la forma establecida en el artículo 29.2 de esta ley"…."g) Efectuar diligencias de prevención y cuantas actuaciones tiendan a evitar la comisión de actos delictivos en el marco de colaboración establecido en las Juntas de Seguridad".

Por su parte, la Ley 4/1992, de 8 de julio, de Coordinación de Policías Locales de la Comunidad de Madrid, también establece como requisito fundamental de los miembros de los Cuerpos de Policía Local la obligación de guardar riguroso secreto respecto a todas las informaciones que conozcan por razón o con ocasión del desempeño de sus funciones. Esta misma ley establece como una de las funciones los Cuerpos de Policía Local en su artículo 53 1.g) efectuar diligencias de prevención y cuantas actuaciones tiendan a evitar la comisión de actos delictivos en el marco de colaboración establecido en las Juntas de Seguridad, teniéndose que comunicar las actuaciones que se practiquen para ello a las Fuerzas y Cuerpos de Seguridad del Estado competentes.

¿Podría la policía local acceder a los datos de menores escolarizados en un Centro educativo?

La policía local, de acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, Reguladora de las Fuerzas y Cuerpos de Seguridad del Estado, y con la Ley 4/1992, de 8 de julio, de Coordinación de Policías Locales de la Comunidad de Madrid, puede ejercer funciones de policía judicial, así como efectuar diligencias de prevención y cuantas actuaciones tiendan a evitar la comisión de actos delictivos en el marco de colaboración establecido en las Juntas de Seguridad.
Se recoge por tanto una especialidad justificada al regular la recogida y tratamiento por parte de las Fuerzas y Cuerpos de Seguridad de datos de carácter personal para fines policiales, en los supuestos en que dicha recogida y tratamiento no cuente con el consentimiento de las personas afectadas. En esos casos, el responsable del fichero, habrá de responder a la solicitud de información que harán los miembros de la policía local, siempre que la petición se realice de forma concreta y específica, al no ser compatible el ejercicio de solicitudes masivas de datos. La petición habrá de recoger igualmente la debida motivación y contemplar el cumplimiento del apartado 4 del mismo artículo 22 de la LOPD, según el cual los datos han de ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.
Por otra parte, la Disposición Adicional Quinta de la Ley Orgánica 4/2000, de 11 de enero, reguladora de los derechos y libertades de los extranjeros en España y su integración social, a partir de la reforma introducida por la Ley Orgánica 14/2003, de 20 de noviembre, en relación con el acceso a la información y colaboración entre Administraciones públicas, establece que:
"1. En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo.
2. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquellos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos."
En el supuesto del centro escolar, el responsable del fichero de datos de menores es el propio centro, que habrá de responder a la solicitud de información que harán los miembros de la policía local, siempre que la petición se realice de forma concreta y específica, al no ser compatible el ejercicio de solicitudes masivas de datos. También

en este caso, la petición habrá de recoger la debida motivación y contemplar el cumplimiento del apartado 4 del mismo artículo 22 de la LOPD.
Las intervenciones por hechos delictivos que realiza la policía local y la obligatoria comunicación de datos por parte de los centros escolares a dicha policía constituirá, en estos casos, una cesión de datos de los menores por parte de centros escolares, tanto públicos como privados, pues esta se define en el artículo 3 i) de la LOPD como "toda revelación de datos realizada a una persona distinta del interesado".
El régimen genérico de las cesiones se encuentra regulado en el artículo 11 de la LOPD y en él se exige el consentimiento del interesado con ciertas excepciones. Sin embargo, la recogida y tratamiento de datos por parte de las Fuerzas y Cuerpos de Seguridad se somete al régimen específico señalado, contenido en el artículo 22 LOPD, cuando realizan actividades de prevención o de represión de infracciones penales.
Además, existe un deber de colaboración con las Fueras y Cuerpos de Seguridad establecido en el artículo 4 de la Ley 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad: "1. Todos tienen el deber de prestar a las Fuerzas y Cuerpos de Seguridad el auxilio necesario en la investigación y persecución de los delitos en los términos previstos legalmente. 2. Las personas y entidades que ejerzan funciones de vigilancia, seguridad o custodia referidas a personal y bienes o servicios de titularidad pública o privada tienen especial obligación de auxiliar o colaborar en todo momento con las Fuerzas y Cuerpos de Seguridad."
De los preceptos citados se desprende la obligación de los centros escolares de facilitar a la policía local los datos necesarios para el desarrollo de sus investigaciones en los términos señalados.

¿Conforme a la LOPD, podría la policía local acceder a los datos de los menores obrantes en un centro educativo para valorar las situaciones de desamparo o cualquier otra situación de riesgo del menor?

El artículo 14 de la Ley Orgánica 1/1996, de 15 enero, de Protección Jurídica del Menor, indica que las autoridades y servicios públicos tienen obligación de prestar la atención inmediata que precise cualquier menor, de actuar si corresponde a su ámbito de competencias o de dar traslado en otro caso al órgano competente y de poner los hechos en conocimiento de los representantes legales del menor, o cuando sea necesario, del Ministerio Fiscal. A su vez, en el artículo 16 de dicha norma se señala que son las entidades públicas competentes en materia de protección de menores las obligadas a verificar y evaluar las situaciones de desprotección que se hayan denunciado, adoptando las medidas necesarias para resolverlas.
El artículo 18 regula las situaciones de desamparo de menores, señalando que cuando la entidad pública competente considere que el menor se encuentra en situación de desamparo actuará en la forma prevista en el artículo 172 y siguientes del Código Civil, asumiendo la tutela de aquél, adoptando las oportunas medidas de protección y poniéndolo en conocimiento del Ministerio Fiscal.
La Comisión de Tutela del Menor es el órgano a través del cual la Comunidad de Madrid ejerce las competencias de protección de los menores, asumiendo su tutela y guarda en virtud de lo establecido en la legislación vigente. El Decreto 198/1998, de 26 de noviembre, regula la composición y funcionamiento de la misma.
Más en concreto, en relación con esta pregunta, debe señalarse lo previsto por los artículos 13 y 17 de la Ley Orgánica 1/1996, de 15 de enero, según los cuales:
"Artículo 13. Obligaciones de los ciudadanos y deber de reserva.
1. Toda persona o autoridad, y especialmente aquellos que por su profesión o función, detecten una situación de riesgo o posible desamparo de un menor, lo comunicarán a

la autoridad o sus agentes más próximos, sin perjuicio de prestarle el auxilio inmediato que precise.
2. Cualquier persona o autoridad que tenga conocimiento de que un menor no está escolarizado o no asiste al centro escolar de forma habitual y sin justificación, durante el período obligatorio, deberá ponerlo en conocimiento de las autoridades públicas competentes, que adoptarán las medidas necesarias para su escolarización.
3. Las autoridades y las personas que por su profesión o función conozcan el caso actuarán con la debida reserva.
En las actuaciones se evitará toda interferencia innecesaria en la vida del menor".
"Artículo 17. Actuaciones en situaciones de riesgo.
En situaciones de riesgo de cualquier índole que perjudiquen el desarrollo personal o social del menor, que no requieran la asunción de la tutela por Ministerio de la Ley, la actuación de los poderes públicos deberá garantizar en todo caso los derechos que le asisten y se orientará a disminuir los factores de riesgo y dificultad social que incidan en la situación personal y social en que se encuentra y a promover los factores de protección del menor y su familia.
Una vez apreciada la situación de riesgo, la entidad pública competente en materia de protección de menores pondrá en marcha las actuaciones pertinentes para reducirla y realizará el seguimiento de la evolución del menor en la familia".
Ello no obstante, el artículo 17 de la Ley 18/1999, de 29 de abril, reguladora de los Consejos de Atención a la Infancia y la Adolescencia de la Comunidad de Madrid, crea el Sistema de Información para la Protección de los Menores, con el objeto de disponer de la información necesaria, a fin de permitir un adecuado conocimiento y planificación de los recursos, así como un correcto tratamiento individualizado de los menores en situación de desprotección, constituyendo un medio de apoyo para la toma de decisiones por parte de los Consejos de Atención a la Infancia y la Adolescencia.
En el artículo 18 de dicha Ley, bajo el título "Características y Funcionamiento del Sistema de Información", se establece que el Sistema de Información se basará en el tratamiento automatizado de los datos personales relativos a menores en situación de desprotección y su administración y acceso estará restringido a los Servicios Sociales de titularidad pública. El titular de la Consejería con competencia en materia de Servicios Sociales, podrá establecer convenios de colaboración con los Municipios titulares de Servicios Sociales, con el fin de ordenar las características técnicas del Sistema de Información, así como las fórmulas de financiación del mismo más adecuadas. Con carácter general, el Sistema de Información para la Protección de los Menores, se regirá por lo establecido en la LOPD.
En consecuencia, si bien de la normativa señalada se deduce la existencia de una habilitación legal suficiente, establecida por medio de una norma con rango de Ley formal, que posibilitaría la cesión inconsentida de los datos personales a los que se refiere la pregunta, amparando el acceso por parte de la Policía Local a los datos de los menores en situación de desamparo o riesgo social al pretendido fin de prestar el auxilio debido y actuar en la forma prevista, habrá de tenerse en cuenta que dicha comunicación de datos debe tener por objeto último el conocimiento de la información relativa al menor por parte de los Servicios Sociales de titularidad pública.
A su vez, dada la remisión realizada por el artículo 18 de la Ley 18/1999, de 29 de abril, reguladora de los Consejos de Atención a la Infancia y la Adolescencia de la Comunidad de Madrid, a la normativa sobre protección de datos, la conformidad de la referida comunicación de datos a la policía local, con funciones específicas de protección de menores, únicamente se ajustaría a los requisitos del denominado "principio de calidad de datos", recogido por el artículo 4 LOPD, cuando los datos cedidos resulten "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido

(artículo 4.1)", no pudiendo usarse "para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos (artículo 4.2)".
Además, debe tenerse en cuenta que, en el caso de los centros escolares, no podría aplicarse el artículo 22.2 de la LOPD, pues éste se refiere a las actividades de la policía dirigidas a la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, mientras que la pregunta planteada se refiere a las actividades dirigidas a detectar situaciones de desamparo de menores. Por ello, procede aplicar el régimen general de las cesiones, establecido en el artículo 11 de la LOPD.
De esta manera, la regla general es el consentimiento, salvo las excepciones previstas en el artículo 11.2, de las cuales interesa a los efectos de esta pregunta la del apartado a): "Cuando la cesión está autorizada por una Ley". Dicha excepción legal está constituida en el caso que nos ocupa por el artículo 13 de la Ley 1/1996, de 15 de enero, de Protección Jurídica del Menor, que señala que toda persona o autoridad, y especialmente aquellos que por su profesión o función, detecten una situación de riesgo o posible desamparo de un menor, lo comunicarán a la autoridad o sus agentes más próximos, sin perjuicio de prestarle el auxilio inmediato que precise. Además, según dicho artículo, cualquier persona o autoridad que tenga conocimiento de que un menor no está escolarizado o no asiste al centro escolar de forma habitual y sin justificación, durante el período obligatorio, deberá ponerlo en conocimiento de las autoridades públicas competentes, que adoptarán las medidas necesarias para su escolarización.
Por tanto, la cesión de datos de los menores por parte de los directores de los centros escolares a la policía local cuando interviene en situaciones de desprotección social de los menores no requiere el consentimiento de estos últimos y es obligatoria en cumplimiento de la Ley 1/1996, de 15 de enero. Dicha cesión puede producirse por requerimiento de la policía local a los centros escolares o por la propia iniciativa de éstos cuando observen situaciones de riesgo social y lo pongan en conocimiento de la policía local.

¿Sería conforme a la LOPD que un centro educativo elaborase un informe a petición de la Policía Local para valorar la situación socio-familiar del menor en supuestos tales como el de desamparo o en relación con cualquier otra situación de riesgo?

A la pregunta concreta de si un centro educativo podría elaborar un informe a petición de la Policía Local a fin de obtener datos relevantes para el conocimiento y valoración de una situación socio-familiar del menor, como pudiera ser el desamparo o cualquier otra situación de riesgo, habría que contestar en sentido negativo. Esta situación no estaría dentro de los casos recogidos en el artículo 22 de la LOPD, ni tampoco contaría con el amparo legal previsto en el artículo 11.2, según el cual la comunicación de datos de carácter personal estaría exenta del deber de solicitar el consentimiento de los interesados si la cesión estuviera autorizada en una ley.
En este sentido, además de lo dispuesto en los artículos 13, 14 y 18 de la Ley Orgánica 1/1996, de 15 enero, de Protección Jurídica del Menor, debe señalarse que el artículo 172 del Código Civil indica que la entidad pública a la que, en el respectivo territorio, esté encomendada la protección de los menores, cuando constate que un menor se encuentra en situación de desamparo, tiene por ministerio de la Ley la tutela del mismo y deberá adoptar las medidas de protección necesarias para su guarda, poniéndolo en conocimiento del Ministerio Fiscal, y notificando en legal forma a los padres, tutores o guardadores, en un plazo de cuarenta y ocho horas. Siempre que sea posible, en el momento de la notificación se les informará de forma presencial y de

modo claro y comprensible de las causas que dieron lugar a la intervención de la Administración y de los posibles efectos de la decisión adoptada.
De lo anterior se desprende que, en principio, la Policía Municipal por propia iniciativa no podría solicitar informes a los centros educativos de los menores para la valoración de una situación de desamparo. En todo caso, si tuviera constancia de tal situación debería ser comunicada a la Comisión de Tutela del Menor. Por tanto, conviene reiterar que la competencia sobre este particular reside en la Comisión de Tutela del Menor, que es el órgano a través del cual la Comunidad de Madrid ejerce sus funciones de protección de los menores, asumiendo su tutela y guarda en virtud de lo establecido en la legislación vigente. El Decreto 198/1998, de 26 de noviembre, regula la composición y funcionamiento de la misma.
También debe reiterarse que el artículo 18 de la Ley 18/1999, de 29 de abril, reguladora de los Consejos de Atención a la Infancia y la Adolescencia de la Comunidad de Madrid regula las situaciones de desamparo de menores, señalando que cuando la entidad pública competente considere que el menor se encuentra en situación de desamparo actuará en la forma prevista en el artículo 172 y siguientes del Código Civil, asumiendo la tutela de aquél, adoptando las oportunas medidas de protección y poniéndolo en conocimiento del Ministerio Fiscal.
En conclusión, la Policía Municipal por propia iniciativa y sin perjuicio de prestar el auxilio inmediato que se precise (artículo 13 de la Ley Orgánica 1/1996, de 15 de enero), no podría solicitar directamente informes de los menores a los centros educativos para efectuar por sí misma la valoración de una situación de desamparo. En todo caso, si tuviera constancia de tal situación a través de los mecanismos a los que se ha dado respuesta en las preguntas anteriores, debería comunicarlo a la Comisión de Tutela del Menor, correspondiendo a dicha Comisión la petición del correspondiente informe.

¿Es posible que un centro educativo público facilite a la Asociación de Madres y Padres de Alumnos del Centro (AMPA) los datos personales de los alumnos cuyos padres no son socios de la misma?

De acuerdo con el artículo 11.1 de la LOPD, este tipo de cesión únicamente podría tener lugar para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado, salvo que una ley estableciera lo contrario.
El Real Decreto 1533/1986, de 11 de julio, regula las Asociaciones de Padres de Alumnos, estableciendo en su artículo 5 el procedimiento de admisión de los asociados y señalando que será en todo caso voluntaria y previa solicitud de inscripción. A los asociados no puede exigírseles más requisitos que el de ser padre o tutor del alumno matriculado en el Centro, abonar, en su caso, las correspondientes cuotas, y aceptar expresamente los correspondientes estatutos.
Dicha norma es meramente reglamentaria, por lo que al no existir una norma con rango de Ley formal que establezca excepción alguna, el centro educativo no puede facilitar a la AMPA los datos personales de los alumnos cuyos padres no son socios de la misma, siendo necesario el consentimiento de los padres para que el centro educativo pueda ceder esos datos, ya que esta cesión no se encuentra recogida en ninguna de las excepciones del artículo 11 de la LOPD.

¿Es legítimo el acceso a los informes de Evaluación Pedagógica de los hijos por parte de los padres separados? En su caso, ¿es necesario informar de la solicitud recibida de uno de los padres al otro que tenga la guardia y custodia del hijo?

Según establece el artículo 6 de la LOPD el consentimiento del interesado es pilar fundamental legitimador de todo tratamiento de datos; consentimiento que en el caso de menores o incapaces será otorgado por sus padres o tutores.
En los casos de padres separados, como señala el artículo 162 del Código Civil, los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. La resolución judicial de la separación es la que establece todo lo relativo a la patria potestad y a la guardia y custodia de los hijos, siendo normalmente compartida la primera, y asignada la segunda a uno de los progenitores.
El ejercicio de la patria potestad es determinante para ostentar el ejercicio de la representación legal de los menores y por tanto, para acceder a todos los datos relativos a su evolución educativa, en la que deben participar los padres, según indica la legislación educativa.
La comunicación a los padres de los informes de Evaluación Pedagógica de sus hijos no puede considerarse cesión de datos del menor siempre y cuando éstos ostenten la patria potestad y por tanto su representación legal.
Desde el punto de vista de la legislación de protección de datos, no existe motivo alguno que impida la solicitud de información por parte de uno de los padres respecto al acceso a dichos informes, siempre que ambos ostenten la patria potestad, condición que deberá acreditarse con la presentación del documento judicial que la establezca (sentencia o auto que aprueben el convenio regulador). Éstos tienen el derecho de acceso a los datos de sus hijos menores en caso de ostentar ambos la patria potestad, en cuanto se erigen en sus representantes legales.
En caso de que uno de los progenitores esté privado judicialmente de la patria potestad del hijo menor, dicha circunstancia deberá quedar acreditada también en el referido documento judicial, ya que en este caso la privación de la patria potestad implicaría la pérdida de la condición de representante legal, no teniendo por tanto acceso a los datos personales del menor sin el consentimiento del otro progenitor.

¿Pueden cederse datos de alumnos inmigrantes para realizar un seguimiento de vacunación de la población residente en la Comunidad de Madrid?

El artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad, y los artículos 15 y 55 de la Ley 12/2001, de 21 de diciembre, de Ordenación Sanitaria de la Comunidad de Madrid, establecen la necesaria prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, con especial énfasis en la vigilancia en salud pública y la difusión de la información epidemiológica general y específica para fomentar el conocimiento detallado de los problemas de salud, como una de las funciones fundamentales de la Administración Sanitaria.
A tal fin, y con sujeción a lo establecido en la norma estatal y autonómica aplicable en materia de protección de datos de carácter personal, los datos relativos a la salud serán cedidos a la Administración Sanitaria de la Comunidad de Madrid por parte de los responsables de los ficheros, cualquiera que sea su titularidad, cuando resulten necesarios para prevención de la enfermedad, o la realización de estudios epidemiológicos.
Por lo tanto, desde el punto de vista de la normativa de protección de datos, la cesión solicitada y referida a los datos de los menores inmigrantes escolarizados puede ser realizada sin la solicitud del consentimiento de los padres de los menores, ya que estaría encuadrada en la excepción del artículo 11.2 a) de la LOPD, según el cual, cuando una ley contemple la cesión, ésta estará exenta del cumplimiento de la norma general del consentimiento de los interesados.
Como se ha expuesto, en este caso la cesión cuenta con el amparo legal del artículo 8 de la Ley General de Sanidad y de los artículos 15 y 55 de la Ley de Ordenación Sanitaria de la Comunidad de Madrid, dado que el objetivo de dicha cesión precisamente consiste en realizar una labor de seguimiento de la situación epidemiológica de la población infantil inmigrante para garantizar una cobertura de vacunación, teniendo competencia para realizar esta función el Instituto de Salud Pública.
No obstante lo anterior, de conformidad con el principio de finalidad recogido en el artículo 4.3 de la LOPD, deberá tenerse en cuenta que los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

¿Es conforme con la LOPD que se informe a los profesores de un Centro Educativo afectados por riesgos para su integridad física y su salud de que un alumno del centro educativo es portador de una grave enfermedad de carácter contagioso?

La comunicación de los datos a los que se refiere la consulta constituye una auténtica cesión de datos, definida por el artículo 3 i) de la LOPD como "Toda revelación de datos realizada a una persona distinta del interesado".
Con carácter general, la comunicación de datos personales quedará sometida a lo dispuesto por el artículo 11.1 de la citada Ley Orgánica, en cuya virtud "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"; esta disposición se ve excepcionada, entre otros supuestos, por lo dispuesto en el apartado 2.a) del propio artículo 11 de la mencionada Ley Orgánica, que posibilita la cesión inconsentida de los datos en caso de que la misma se encuentre fundamentada en lo establecido por una norma con rango de Ley.
De manera concreta, tratándose de datos relacionados con la salud de las personas, el artículo 7.3 de la Ley Orgánica 15/1999 establece que "los datos de carácter

personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente."
Además, el artículo 7.6 de la LOPD ampara la cesión en determinados supuestos a los que se refiere de forma específica, al señalar "No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto", añadiendo que "También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".
A su vez el artículo 8 de la LOPD dispone que "Sin perjuicio de lo que dispone el artículo 11 respecto de al cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad."
En relación con la posible existencia de habilitaciones legales específicas que, basadas en la existencia de una norma con rango de ley formal, amparen la cesión inconsentida del tipo de datos al que se refiere la consulta, conviene traer a colación lo previsto por el artículo 14.1 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, de acuerdo con el cual:
"Los trabajadores tienen derecho a una protección eficaz en materia de seguridad y salud en el trabajo. El citado derecho supone la existencia de un correlativo deber del empresario de protección de los trabajadores frente a los riesgos laborales. Este deber de protección constituye, igualmente, un deber de las Administraciones públicas respecto del personal a su servicio.
Los derechos de información, consulta y participación, formación en materia preventiva, paralización de la actividad en caso de riesgo grave e inminente y vigilancia de su estado de salud, en los términos previstos en la presente Ley, forman parte del derecho de los trabajadores a una protección eficaz en materia de seguridad y salud en el trabajo".
Por su parte, en cuanto a la "información, consulta y participación de los trabajadores", el artículo 18 de la mencionada Ley dispone que:
"1. A fin de dar cumplimiento al deber de protección establecido en la presente Ley, el empresario adoptará las medidas adecuadas para que los trabajadores reciban todas las informaciones necesarias en relación con:
a. Los riesgos para la seguridad y la salud de los trabajadores en el trabajo, tanto aquellos que afecten a la empresa en su conjunto como a cada tipo de puesto de trabajo o función.
b. Las medidas y actividades de protección y prevención aplicables a los riesgos señalados en el apartado anterior.
c. Las medidas adoptadas de conformidad con lo dispuesto en el artículo 20 de la presente Ley.
En las empresas que cuenten con representantes de los trabajadores, la información a que se refiere el presente apartado se facilitará por el empresario a los trabajadores a través de dichos representantes; no obstante, deberá informarse directamente a cada trabajador de los riesgos específicos que afecten a su puesto de trabajo o función y de las medidas de protección y prevención aplicables a dichos riesgos. (…)"

Finalmente, en relación con la posible existencia de un "riesgo grave e inminente", el artículo 21 de la citada Ley 31/1995, de 8 de noviembre, prevé que:
"1. Cuando los trabajadores estén o puedan estar expuestos a un riesgo grave e inminente con ocasión de su trabajo, el empresario estará obligado a:
a. Informar lo antes posible a todos los trabajadores afectados acerca de la existencia de dicho riesgo y de las medidas adoptadas o que, en su caso, deban adoptarse en materia de protección.
b. Adoptar las medidas y dar las instrucciones necesarias para que, en caso de peligro grave, inminente e inevitable, los trabajadores puedan interrumpir su actividad y, si fuera necesario, abandonar de inmediato el lugar de trabajo. En este supuesto no podrá exigirse a los trabajadores que reanuden su actividad mientras persista el peligro, salvo excepción debidamente justificada por razones de seguridad y determinada reglamentariamente.
c. Disponer lo necesario para que el trabajador que no pudiera ponerse en contacto con su superior jerárquico, ante una situación de peligro grave e inminente para su seguridad, la de otros trabajadores o la de terceros a la empresa, esté en condiciones, habida cuenta de sus conocimientos y de los medios técnicos puestos a su disposición, de adoptar las medidas necesarias para evitar las consecuencias de dicho peligro. (…)"
Así, con base en lo dispuesto por los preceptos legales citados, los trabajadores del centro educativo consultante podrían poseer información relativa a las enfermedades contagiosas, a las de riesgo de violencia, y a los estados críticos, tales como drogodependencias o alcoholismos, sin el consentimiento de los afectados. Como regla general, esta información mínima debería proporcionársela la Dirección del centro escolar, independientemente del consentimiento del afectado.
En conclusión, sin necesidad de que concurra el consentimiento del afectado, para el correcto desarrollo de sus propias funciones, los profesores del centro que se encuentren expuestos a una situación de riesgo para su integridad física y/o salud, podrían obtener información acerca de los datos de salud de los alumnos, tales como los relativos a las enfermedades contagiosas que padecen dichos alumnos, siempre que dichos profesores corran el riesgo de contagiarse. Asimismo, podrían tener conocimiento de otros datos referentes a los posibles riesgos de violencia derivados de la naturaleza de su enfermedad, como ocurre en los casos de alcoholismo, drogadicción, perturbaciones mentales como esquizofrenia, o los relativos a otras enfermedades que puedan dar lugar a episodios de violencia.
No obstante lo anterior, el centro educativo deberá estar a lo dispuesto por el artículo 4 de la LOPD en relación con el denominado "principio de calidad de los datos", de acuerdo con el cual "1. Los datos de carácter persona sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2 Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".
De acuerdo con lo anterior, para proceder a la comunicación del dato de salud del alumno (al que ser refiere esta pregunta) a los profesores expuestos a una situación de riesgo, deberá valorarse previamente por el centro educativo la verdadera, efectiva e indudable concurrencia del referido riesgo para la integridad física y/o salud de las personas, sin que pueda considerarse la concurrencia de la habilitación legal a la que se ha hecho cumplida mención en aquéllos supuestos en los que la praxis sanitaria o las recomendaciones de las autoridades competentes en materia de salud pública recomienden la confidencialidad absoluta de dichos datos sanitarios en atención a su

carácter inocuo respecto de terceras personas, o en razón de las características de las formas concretas de contagio de la enfermedad.
A su vez, para el caso de que valorado el supuesto concreto se aprecie la concurrencia del riesgo vital al que se refiere la consulta del centro educativo, deberá garantizarse que, de acuerdo con lo dispuesto por el artículo 10 de la LOPD, y en el artículo 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, quede debidamente asegurado el deber de secreto de todas las personas que conozcan la información de carácter personal relativa al alumno afectado por la enfermedad contagiosa a la que se refiere la consulta.
El incumplimiento de lo previsto en dichos preceptos y/o el uso de los datos de carácter personal obtenidos por los profesores para finalidades distintas de las preventivas en relación con su salud e integridad física, podría dar lugar, en su caso, a la incoación del correspondiente expediente sancionador por parte de la autoridad de control competente por infracción de lo dispuesto por la LOPD, y a la imposición -en su caso- de las sanciones previstas por dicha norma en su Título VII, que prevé la imposición de multas que ascienden hasta los 300.000 euros.

¿Es conforme con la LOPD que la Administración educativa requiera la cumplimentación de determinados datos de carácter personal correspondientes a los alumnos de un Centro Educativo relativos a la circunstancia de ser gitano? En caso afirmativo ¿De qué modo debe procederse para confirmar que una persona determinada es de raza gitana? ¿Resulta conforme con la normativa sobre protección de datos la petición de documentación acreditativa de dicha pertenencia étnica y/o racial? ¿En el supuesto de menores de edad, el dato correspondiente debe recabarse del propio menor o de sus padres o tutores?

En primer lugar, es necesario analizar la posible existencia de normas específicas que legitimen el tratamiento por parte de la Administración educativa de la Comunidad de Madrid de los datos de carácter personal relativos a la pertenencia de los alumnos a la etnia gitana, legitimando -asimismo- el requerimiento de dichos datos de carácter personal, relativos a "la circunstancia de ser gitano" a los centros educativos.
El artículo 7.3 de la LOPD dispone que "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente." Por tanto, la Administración educativa sólo podrá requerir y tratar el dato de la pertenencia a la etnia gitana cuando una ley lo prevea, en defecto del consentimiento expreso del afectado.
El legislador educativo, tanto estatal como autonómico, considera que la pertenencia de los alumnos a ciertas etnias puede dar lugar a necesidades educativas especiales a las que la Administración educativa deberá atender. Por ello, la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en su artículo 80 señala lo siguiente:
"1. Con el fin de hacer efectivo el principio de igualdad en el ejercicio del derecho a la educación, las Administraciones públicas desarrollarán acciones de carácter compensatorio en relación con las personas, grupos y ámbitos territoriales que se encuentren en situaciones desfavorables y proveerán los recursos económicos y los apoyos precisos para ello.
2. Las políticas de educación compensatoria reforzarán la acción del sistema educativo de forma que se eviten desigualdades derivadas de factores sociales, económicos, culturales, geográficos, étnicos o de otra índole.
3. Corresponde al Estado y a las Comunidades Autónomas en sus respectivos ámbitos de competencia fijar sus objetivos prioritarios de educación compensatoria."

En el ámbito de la Comunidad de Madrid, la Resolución de 21 de julio de 2006, de la Viceconsejería de Educación, por la que se dictan Instrucciones para la organización de las actuaciones de compensación educativa en el ámbito de la enseñanza básica en los centros docentes sostenidos con fondos públicos de la Comunidad de Madrid, señala en su Norma Tercera que son destinatarios de la compensación educativa "el alumnado escolarizado en educación primaria y en educación secundaria obligatoria que se encuentre en situación de desventaja socioeducativa por su pertenencia a minorías étnicas y/o culturales, por factores sociales, económicos o geográficos, y presente desfase escolar significativo, con dos o más cursos de diferencia entre su nivel de competencia curricular y el curso en el que está escolarizado, así como dificultades de inserción educativa y necesidades de apoyo específico derivadas de la incorporación tardía al sistema educativo o por una escolarización irregular.

En cuanto a la etnia gitana en concreto, la Ley 4/2002, de 27 de junio, de Creación de la Mesa para la Integración y Promoción del pueblo gitano de la Comunidad de Madrid, también reconoce las necesidades educativas especiales de la etnia gitana en su artículo 4:

"Las informaciones objeto de tratamiento por parte de la Mesa y susceptibles de incorporarse al Plan de Actuación al que se refiere el artículo 3.1 de la presente Ley, tratarán de las siguientes materias: (…) c) Educación, en todo lo relativo al desarrollo de acciones complementarias para apoyar la integración del alumnado gitano (programas específicos de mediación, seguimiento escolar y apoyo, en colaboración con entidades sociales; fomento de la incorporación temprana del alumnado gitano a la educación infantil; programas dirigidos a la mejora del rendimiento del alumnado gitano en educación primaria; acciones orientadas a apoyar la transición del alumnado a la educación secundaria obligatoria; programas de desarrollo de espacios socioeducativos con alumnado gitano fuera del centro escolar), a la promoción de la participación de padres y madres de etnia gitana en AMPAS (Asociaciones de Madres y Padres de Alumnos) y en Consejos Escolares, así como a la formación de personas adultas de etnia gitana."

En consecuencia, con arreglo a las normas anteriores, la Administración educativa puede requerir y tratar el dato de la pertenencia a la etnia gitana, pues existen leyes y normas de rango inferior que, atendiendo al interés general de lograr una educación equitativa, disponen que se atiendan las necesidades concretas de los grupos sociales y etnias y, en concreto, de la etnia gitana.

En relación con la última cuestión planteada, esto es, la relativa a la exigencia de documentación acreditativa de la pertenencia a la etnia gitana, en caso de existir dicha documentación, la exigencia de la misma resultaría conforme a la normativa de protección de datos, ya que el requerimiento y tratamiento del dato en cuestión está amparado por las normas mencionadas anteriormente y es lógico que la Administración educativa trate de comprobar la veracidad de los datos, puesto que los mismos permiten valorar las necesidades educativas de los alumnos y pueden dar lugar o no a acciones complementarias.

Ello no obstante, el centro consultante habrá de estar a lo dispuesto por el artículo 4.1 de la LOPD, relativo al denominado "principio de calidad de datos" y, en concreto, al principio de proporcionalidad en la exigencia de los mismos. Así, de acuerdo con dicho precepto:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

En consecuencia, en relación con la constatación y verificación de este tipo de dato, y a salvo la posibilidad de su acreditación documental, a nuestro juicio, resultaría desproporcionado y contrario al mencionado principio de calidad la exigencia de

cualquier tipo de reconocimiento médico o examen físico y/o clínico en orden a la comprobación de la pertenencia de un individuo a una determinada raza o minoría etnia.
A dichos efectos, debería considerarse como válida la propia manifestación del afectado o, en su caso, de sus padre, madre o tutor, sin que sea menester la exigencia de ningún tipo de prueba o acta adicional que sirva para acreditar la "notoriedad" y "certeza" de dicha declaración.
En cuanto a si los datos "de origen racial", tratándose de menores de edad, deben recabarse de los propios menores o de sus padres o tutores, para los menores de dieciséis años dichos datos deberán solicitarse y obtenerse del padre, madre o tutor legal, pudiendo solicitarse directamente de los propios alumnos dichos datos "sobre pertenencia a una etnia o raza" sólo en el supuesto de los mayores de dieciséis años.
Así, de una parte, en relación con la solicitud de los datos directamente de los alumnos, menores de edad, será necesario analizar la normativa aplicable para determinar en qué supuestos los mismos ostentan la capacidad necesaria para prestar este consentimiento "específico" en relación con datos de "origen racial", y en cuáles deberá solicitarse dicho consentimiento de su representante legal.
Con carácter general, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta en relación con una parte importante de los supuestos que pueden plantearse en el ámbito educativo, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 para los mayores de catorce años.
Además, también con carácter general, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en Resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.
Refrendando esta tesis -de tipo general-, el artículo 13 del nuevo Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD, establece que:
"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y

dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales".
En consecuencia, a tenor de las normas referidas, cabría considerar -inicialmente- que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. Respecto de los restantes menores de edad, debería estarse a lo dispuesto en el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD.
Sin embargo, en el supuesto de menores de edad que no hayan cumplido los dieciséis años, existen argumentos jurídicos que apuntan claramente en orden a la necesaria solicitud del consentimiento del padre, madre o tutor para la obtención de la información "de origen racial" a la que se refiere el supuesto objeto de la pregunta.
Así, por una parte, el citado artículo 13.1 del Real Decreto 1720/2007, de 21 de diciembre, ha establecido -por vía de excepción- la posibilidad de que la Ley exija para la prestación del consentimiento al tratamiento de los datos la asistencia de los titulares de la patria potestad o tutela. Pues bien, en todos estos casos -en los que la Ley así lo exija- se deduciría la necesidad del consentimiento del padre, madre o tutor.
En lo que afecta a la pregunta relativa al "origen racial" del menor, tal y como se ha adelantado, a juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, debe concluirse que la obtención de dicho tipo de datos -especialmente protegidos- relativos a menores de dieciséis años, deberá obtenerse de los representantes legales del menor, pudiendo recabarse del menor directamente sólo en el supuesto de los mayores de dieciséis años. Esto es, hasta que el menor no tenga dieciséis años cumplidos deberá solicitarse -en su caso- la información de "origen racial" de sus padres o de sus representantes legales, dado que se trata de una cuestión de trascendental importancia para el menor, consustancial al ejercicio de la patria potestad, requiriendo directamente la información del menor sólo en el supuesto de los mayores de dieciséis años.
Por otra parte, abonando esta tesis -mantenida por la Agencia de Protección de Datos de la Comunidad de Madrid-, existen importantes normas sectoriales específicas. Así, la Ley de la Comunidad de Madrid 5/2002, de 27 de junio, de Drogodependencia, señala que "en el caso de que un menor de dieciséis años precise atención sanitaria por consumo de bebidas alcohólicas u otras drogas, los centros o servicios sanitarios que presten atención, deberán comunicar la situación del menor a los padres o tutores para que éstos se hagan cargo del menor. Asimismo, también se pondrá en conocimiento de dichos padres o tutores cuando fuese menor de dieciocho años y la situación, a juicio del facultativo, pudiera considerarse de gravedad". Este precepto establece la misma franja de edad que el art. 9.3 c) de la Ley 41/2002, de 14 de noviembre, de "autonomía del paciente", que establece la obligación de informar a los padres de menores emancipados o con dieciséis años cumplidos "en caso de actuación de grave riesgo, según el criterio del facultativo".
A su vez, específicamente en materia educativa, el artículo 4 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, dispone que "1. La enseñanza básica a la que se refiere el artículo 3.3 de esta Ley es obligatoria y gratuita para todas las personas. 2. La enseñanza básica comprende diez años de escolaridad y se desarrolla, de forma regular, entre los seis y los dieciséis años de edad". Por su parte, en el artículo 22 de

dicha Ley Orgánica se establece que "La etapa de educación secundaria obligatoria comprende cuatro cursos, que se seguirán ordinariamente entre los doce y los dieciséis años de edad".
Dichos preceptos deben ponerse en relación con lo previsto en la legislación sobre protección del menor, contenida en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, en cuyo artículo 2 (Principios generales), se establece que "En la aplicación de la presente Ley primará el interés superior de los menores sobre cualquier otro interés legítimo que pudiera concurrir. Asimismo, cuantas medidas se adopten al amparo de la presente Ley deberán tener un carácter educativo. Las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva".
En conclusión, a juicio de la APDCM no resultaría conforme con la LOPD que el dato relativo al "origen racial" de los menores de dieciséis años se solicitase y obtuviera directamente del menor, debiendo -en consecuencia- requerirse dicha información del padre, madre o tutor del mismo.
En el supuesto de los mayores de dieciséis años, nada se opone a la posibilidad de que el mencionado dato se obtenga directamente del menor en aplicación de lo dispuesto en el artículo 4 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, y en el artículo 2 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.
Por tanto, a la vista de lo anteriormente señalado, será necesario recabar el consentimiento de los menores (mayores de dieciséis años) o de sus representantes legales (menores de dieciséis años) para la recogida de sus datos de origen racial, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley Orgánica, recabándose, en el caso de menores de dieciséis años el consentimiento de sus representantes legales.
En resumen, los datos personales objeto de esta pregunta deberán ser recabados del padre, madre o tutor legal cuando el alumno sea menor de dieciséis años.
Así, de acuerdo con lo dispuesto por el artículo 22 (principios generales) de la Ley Orgánica 2/2006, de 3 mayo, de Educación, "1. La etapa de educación secundaria obligatoria comprende cuatro cursos, que se seguirán ordinariamente entre los doce y los dieciséis años de edad", correspondiendo a "los padres que ostenten la patria potestad la representación legal de sus hijos menores no emancipados (artículo 162 del Código Civil)".
A mayor abundamiento, la Disposición Adicional Vigésimo Tercera (Datos personales de los alumnos) de la referida Ley Orgánica 2/2006, de 3 mayo, de Educación, establece que:
"1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.
2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.
3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto

del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.
4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal, y las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas en el seno de la Conferencia Sectorial de Educación".
Finalmente, en relación con el alumnado con necesidad específica de apoyo educativo, el artículo 71 de la mencionada Ley Orgánica (Principios), establece que
"1. Las Administraciones educativas dispondrán los medios necesarios para que todo el alumnado alcance el máximo desarrollo personal, intelectual, social y emocional, así como los objetivos establecidos con carácter general en la presente Ley.
2. Corresponde a las Administraciones educativas asegurar los recursos necesarios para que los alumnos y alumnas que requieran una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar, puedan alcanzar el máximo desarrollo posible de sus capacidades personales y, en todo caso, los objetivos establecidos con carácter general para todo el alumnado.
3. Las Administraciones educativas establecerán los procedimientos y recursos precisos para identificar tempranamente las necesidades educativas específicas de los alumnos y alumnas a las que se refiere el apartado anterior. La atención integral al alumnado con necesidad específica de apoyo educativo se iniciará desde el mismo momento en que dicha necesidad sea identificada y se regirá por los principios de normalización e inclusión.
4. Corresponde a las Administraciones educativas garantizar la escolarización, regular y asegurar la participación de los padres o tutores en las decisiones que afecten a la escolarización y a los procesos educativos de este alumnado. Igualmente les corresponde adoptar las medidas oportunas para que los padres de estos alumnos reciban el adecuado asesoramiento individualizado, así como la información necesaria que les ayude en la educación de sus hijos".
En consecuencia, de la citada normativa se extrae la obligación de los padres, madres y tutores legales, que ostenten la patria potestad, de velar por la escolarización de sus hijos durante todo el periodo de escolarización obligatoria (dieciséis años), siendo que dicha obligación queda refrendada específicamente en relación con el aseguramiento de la escolarización de los menores en el supuesto de que concurran necesidades específicas de apoyo educativo.

¿Resulta conforme con lo dispuesto en la LOPD el tratamiento de los datos de salud de los alumnos con discapacidad para llevar a cabo las correspondientes "adaptaciones curriculares", sin recabar para ello el consentimiento de los alumnos, padres o tutores?

Según se expone en la pregunta, el tratamiento de dichos datos resulta necesario para garantizar la escolarización e integración del alumnado, por lo que, de acuerdo con lo dispuesto por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, podría resultar suficiente para la cesión de los mismos la simple "información" a los afectados, sin necesidad de recabar su consentimiento.
A la consulta se acompañan dos modelos-tipo relativos a la "solicitud de adaptación curricular" solicitada por el padre-madre o tutor del alumno al centro escolar, y al "certificado médico", expedido por facultativo, en el que deben cumplimentarse determinados datos de salud del alumno que requiera la correspondiente adaptación.

La especial protección conferida a los datos relacionados con la salud de las personas no es arbitraria, sino que resulta de lo dispuesto en las normas Internacionales y Comunitarias reguladoras del tratamiento automatizado de datos de carácter personal. En este contexto, tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, así como el artículo 6 del Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección, de tal forma que, como indica el citado Convenio, tales datos "no podrán tratarse automatizadamente a menos que el derecho interno prevea garantías adecuadas."

La Organización Mundial de la Salud en su Carta Magna (1946) definió la salud como "el estado de completo bienestar físico, mental o social, y no solamente la ausencia de afecciones o enfermedades".

El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa, sobre protección de los derechos de las personas en lo que se refiere al tratamiento de sus datos viene a definir la noción de "datos de carácter personal relativos a la salud", considerando que su concepto abarca "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo", pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que "debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas".

En la Recomendación nº R (97) 5, adoptada por el Comité de Ministros del 13 de febrero de 1997, relativa a protección de datos médicos, se determina que la expresión "datos médicos" hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas.

Finalmente, el artículo 5.1 g) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define los "Datos de carácter personal relacionados con la salud", señalando que se trata de "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética".

En consecuencia, de las previsiones legales expuestas se desprende nuevamente que el concepto de datos relacionados con la salud de las personas no hace referencia a una situación temporal, sino también permanente, de las personas, puesto que afecta a su situación pasada, presente o futura, siendo así que la falta permanente de plenitud en el estado de salud también guarda relación con la misma.

La información a la que se refiere la pregunta contendría datos de carácter personal relacionados con la salud de los alumnos, toda vez que los problemas, trastornos y enfermedades padecidas por los mismos son los que, en su caso, justificarían la existencia de "adaptaciones curriculares" determinadas.

En el artículo 7 de la LOPD se establece que la información más sensible, que afecta en mayor medida a la intimidad y privacidad de las personas y al ejercicio de los derechos fundamentales consagrados por la Constitución, sea objeto de una protección reforzada, que pasa, en la mayor parte de los supuestos, por la exigencia del consentimiento del afectado para su tratamiento.

En concreto, según dispone el artículo 7.3 de la Ley Orgánica 15/1999, "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una Ley o el afectado consienta expresamente". En consecuencia, los datos a los que se refiere la consulta sólo podrían comunicarse en caso de que así se hubiera consentido por los propios alumnos o su representante legal o cuando una Ley

lo dispusiera, siendo así que en la consulta realizada no se desprende la existencia de dicha norma habilitadora de la comunicación de estos datos.
Si se siguiese la tesis formulada en la consulta, esta especial protección quedaría vacía de contenido, procediéndose a la recogida y cesión de los datos de salud de los alumnos afectados sin el consentimiento expreso de estos. En este sentido, conviene traer a colación la regulación contenida en los artículos 71 y 72 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, en la que el consultante pretende justificar el tratamiento inconsentido de los datos de salud de los alumnos.
De acuerdo con dichos artículos:
"Artículo 71. Principios.
1. Las Administraciones educativas dispondrán los medios necesarios para que todo el alumnado alcance el máximo desarrollo personal, intelectual, social y emocional, así como los objetivos establecidos con carácter general en la presente Ley.
2. Corresponde a las Administraciones educativas asegurar los recursos necesarios para que los alumnos y alumnas que requieran una atención educativa diferente a la ordinaria, por presentar necesidades educativas especiales, por dificultades específicas de aprendizaje, por sus altas capacidades intelectuales, por haberse incorporado tarde al sistema educativo, o por condiciones personales o de historia escolar, puedan alcanzar el máximo desarrollo posible de sus capacidades personales y, en todo caso, los objetivos establecidos con carácter general para todo el alumnado.
3. Las Administraciones educativas establecerán los procedimientos y recursos precisos para identificar tempranamente las necesidades educativas específicas de los alumnos y alumnas a las que se refiere el apartado anterior. La atención integral al alumnado con necesidad específica de apoyo educativo se iniciará desde el mismo momento en que dicha necesidad sea identificada y se regirá por los principios de normalización e inclusión.
(…)"
"Artículo 72. Recursos.
"1. Para alcanzar los fines señalados en el artículo anterior, las Administraciones educativas dispondrán del profesorado de las especialidades correspondientes y de profesionales cualificados, así como de los medios y materiales precisos para la adecuada atención a este alumnado.
(…)
3. Los centros contarán con la debida organización escolar y realizarán las adaptaciones y diversificaciones curriculares precisas para facilitar a todo el alumnado la consecución de los fines establecidos.
4. Las Administraciones educativas promoverán la formación del profesorado y de otros profesionales relacionada con el tratamiento del alumnado con necesidad específica de apoyo educativo.
(…)"
Pues bien, de lo dispuesto en los preceptos citados no se extrae la existencia de habilitación alguna que ofrezca cobertura al tratamiento inconsentido de los datos de salud de los alumnos. Esto es, la recogida, tratamiento y cesión inconsentida de dichos de salud de las personas no encuentra amparo en la citada Ley Orgánica 2/2006, de 3 de mayo, de Educación, sin que resulte admisible que la mera atribución genérica de competencias, la descripción de funciones legales o la determinación legal de las obligaciones de los centros y/o del profesorado resulte suficiente para considerar válido el tratamiento inconsentido de dichos datos.
En conclusión, sin perjuicio de la obligación de "información" en la recogida de los datos, a la que se hace mención en la pregunta (artículo 5 de la LOPD), deberá procederse, en todo caso, a recabar el consentimiento expreso de las personas afectadas en relación con la recogida de sus datos de salud.

Asimismo, y de conformidad con el artículo 4 de la LOPD, en el supuesto de que se facilitasen datos personales, siempre y cuando exista consentimiento expreso y previo para la comunicación de los mismos, los datos que se recaben deberán ser adecuados, pertinentes y no excesivos para la finalidad para la cual se recaban, debiendo ser cancelados o borrados cuando hayan dejado de ser necesarios para la finalidad que motivo dicha recogida.
Finalmente, en la pregunta se señala que "los profesores -a veces- cedemos información requerida (de capacidades, actitudes, etcétera, de cierto alumnado) por parte de personas u organismos sin identificar, sin poner impedimentos al respecto", por lo que se plantea "¿si pueden negarse a ceder dicha información de los alumnos a organismos, entidades y personas sin identificar?"
En relación con esta cuestión, no cabe sino reiterar que, de acuerdo con lo dispuesto por el artículo 11.1 de la LOPD, "Los datos de carácter personal objeto de tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado".
En consecuencia, el profesor que formula la pregunta no sólo puede, sino que, de acuerdo con el citado precepto, debe abstenerse de realizar cesiones de datos de carácter personal, salvo que concurra el consentimiento señalado, o bien se dé alguno de los supuestos de excepción recogidos en el apartado 2 del mencionado artículo 11 de la LOPD. En este sentido, debe recordarse que "La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas" constituye una infracción muy grave, recogida por el artículo 44.4 b) de la citada LOPD. Asimismo, también puede suponer una vulneración del deber de secreto, infracción tipificada como leve por el artículo 44.2 e) de la LOPD y como muy grave por el artículo 44.4.g) de la LOPD en el caso de que afecte a datos de salud.

¿Es conforme con la LOPD la solicitud de la Secretaría General Técnica de la Consejería de Educación a los centros docentes públicos y privados de determinados datos personales de alumnos graduados en un determinado curso en las enseñanzas de Educación Secundaria y de Formación Profesional, y de alumnos que abandonaron la ESO?

Atendiendo a la legislación específica en materia de estadística pública, el artículo 8 de la Ley 12/1989, de 9 mayo, de la Función Estadística Pública (LFEP en adelante) señala que el Plan Estadístico Nacional, que será aprobado por Real Decreto y tendrá una vigencia de cuatro años, es el principal instrumento ordenador de la actividad estadística de la Administración del Estado. El Real Decreto por el que se aprueba dicho Plan tendrá que especificar las estadísticas que han de elaborarse en el cuatrienio por los servicios de la Administración General del Estado o cualesquiera otras entidades dependientes de la misma y las que hayan de llevarse a término total o parcialmente con la participación de las Comunidades Autónomas o las Corporaciones Locales. El Gobierno elaborará un Programa anual que será aprobado por Real Decreto, conteniendo las actuaciones que hayan de desarrollarse en ejecución del Plan Estadístico Nacional.
El artículo 149.1.31 de la Constitución Española señala que el Estado tiene competencia exclusiva sobre la estadística para fines estatales, y según el artículo 9.1 de la LFEP tendrán consideración de estadísticas para fines estatales las reguladas en el artículo 8 de la propia ley, es decir, las que componen el Plan Estadístico Nacional.
El artículo 7.1 de la LFEP señala que las estadísticas para cuya elaboración se exijan datos con carácter obligatorio se establecerán por Ley, y a tal efecto, la Disposición Adicional Cuarta de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990, modificada por la Disposición Adicional Segunda de la Ley 13/1996,

de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, establece las estadísticas de cumplimentación obligatoria:
"Uno. De conformidad con lo establecido en el artículo 7 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, se consideran estadísticas de cumplimentación obligatoria las siguientes:
(…)
y) Las estadísticas que formen parte del Plan Estadístico Nacional y específicamente según el artículo 45.2 de la, de la Función Estadística Pública, aquellas cuya realización resulte obligatoria para el Estado español por exigencia de la normativa de la Unión Europea. Asimismo, las estadísticas que pudieran realizarse al amparo del artículo 8.3 de la citada Ley.
Todo ello sin perjuicio de lo establecido en el punto 2 del artículo 11 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública.
Dos. Para dichas estadísticas, los organismos que deben intervenir en su elaboración, el enunciado de sus fines y la descripción general de su contenido, el colectivo de personal y el ámbito territorial de referencia, así como la estimación de los créditos presupuestarios necesarios para su financiación, serán los especificados en el Plan Estadístico Nacional."
La Encuesta de Transición/Inserción en el Mercado Laboral forma parte del Plan Estadístico Anual 2001-2004, aprobado por el Real Decreto 1126/2000, de 16 de junio.
El artículo 2 Real Decreto 125/2004, de 23 de enero, por el que se aprueba el Programa Anual 2004 del Plan Estadístico Nacional 2001-2004, que regula el contenido del programa y obligatoriedad de respuesta, establece que:
"1. El Programa anual 2004 contiene las estadísticas para fines estatales que han de llevarse a cabo en dicho año por los servicios de la Administración General del Estado o cualesquiera otras entidades dependientes de ella.
2. Las estadísticas incluidas en el Programa anual 2004 son de cumplimentación obligatoria, sin perjuicio de que serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los interesados los datos susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar".
Siendo el Instituto Nacional de Estadística (INE) el organismo responsable de la Encuesta de Transición/Inserción en el Mercado Laboral, el Anexo II del citado Real Decreto 125/2004 indica que en su elaboración participarán también las Comunidades Autónomas, el Ministerio de Educación y Cultura y Deportes y el Ministerio de Trabajo y Asuntos Sociales.
Según dispone la LOPD en su artículo 2.3 b) los ficheros que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública, se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por la propia LOPD.
El artículo 11.1 de la LOPD regula la comunicación de datos, es decir, toda revelación de datos realizada a una persona distinta del interesado, estableciendo que los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. Es decir, la norma general para que tenga lugar una cesión de datos es que los afectados manifiesten su consentimiento, y que dicha comunicación persiga un fin legítimo entre cedente y cesionario.
No obstante, dicha norma general no es absoluta y así el propio artículo 11 regula una serie de excepciones en su apartado segundo, y de esta manera, el consentimiento no será preciso cuando la cesión se produzca entre Administraciones Públicas y tengo

por objeto el tratamiento posterior de los datos con fines históricos, estadísticos y científicos.
También se encuentran excepciones a la norma del consentimiento en el artículo 21 de la LOPD, según el cual no sería preciso el consentimiento de los interesados para que tuviera lugar la comunicación de datos entre dos Administraciones para el ejercicio de las mismas competencias o cuando la comunicación tuviera por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
A la vista de las citadas normas, hay que concluir que la Encuesta de Transición/Inserción en el Mercado Laboral forma parte del Plan Estadístico Anual 2001-2004, y su cumplimentación es obligatoria según disponen el artículo 7.1 de la LFEP en relación con la Disposición Adicional Cuarta de la Ley 4/1990, de 29 de junio, de Presupuestos Generales del Estado para 1990, modificada por la Disposición Adicional Segunda de la Ley 13/1996, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social, por lo que será obligatorio facilitar por parte de los colegios los datos solicitados para llevar a cabo la elaboración de la encuesta, no siendo dicha comunicación contraria a la LOPD, dado que -precisamente- tal como se ha analizado anteriormente, una de las excepciones para que dicha comunicación tenga lugar, es la posibilidad de que una ley expresamente regule la misma, como se produce en el presente supuesto.
Por otra parte el hecho de que sea la Consejería de Educación de la Comunidad de Madrid la que recabe la información necesaria para el desarrollo de la encuesta por parte del INE, estaría amparado con carácter general en el artículo 3.2 de la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, según el cual Administraciones Públicas, en sus relaciones, se han de regir por el principio de colaboración y cooperación.

¿Conforme a la LOPD qué tipo de acceso a documentación con datos personales deberán tener los equipos de orientación educativa y psicopedagógica?

En primer lugar, se puede señalar que la actividad de estos equipos tiene un encaje legal muy específico que deriva de la garantía de dos derechos constitucionales, como son, de una parte, el derecho a la educación reconocido en el artículo 27 CE, y de otra, el derecho que tienen los discapacitados físicos, sensoriales y psíquicos, reconocido en el artículo 49 CE, a no verse discriminados en el cumplimiento, respecto de ellos, de todos los derechos constitucionales.
De conformidad con estas previsiones constitucionales, el acceso y el procedimiento de adaptación de los discapacitados físicos, psíquicos o sensoriales al sistema educativo fue regulado primero en la Ley Orgánica 1/1990, de 3 de octubre de Ordenación General del Sistema Educativo, más tarde por la Ley Orgánica 10/2002, de 23 de diciembre de Calidad de la Educación, y actualmente por la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que han sido objeto de los correspondientes desarrollos reglamentarios.
Las citadas disposiciones legales y reglamentarias inciden en la actividad específica de los equipos de orientación, y por lo que se refiere a la adecuación de esta actividad a la protección de datos de carácter personal -y atendiendo a las obligaciones que establece la LOPD-, se analizan a continuación de forma general aquellas dudas que se han planteado.
En primer lugar, hay que señalar que el ámbito de la LOPD está centrado en la necesaria existencia de ficheros manuales estructurados o informatizados para el ejercicio de la actividad y es ahí donde incide el cumplimiento de los principios y derechos que la ley enmarca. Así y empezando por quien es el responsable del fichero y quien tendría que declararlo, la propia Ley Orgánica define al responsable del fichero

o tratamiento como la persona física o jurídica u órgano administrativo que decida sobre la finalidad, uso y contenido del tratamiento.
De acuerdo con la normativa específica que regula la actividad de los equipos, queda muy bien definido que los responsables de la evaluación psicopedagógica de los alumnos serán los equipos de orientación educativa o psicopedagógica y los departamentos de orientación de los centros docentes. En consecuencia, toda la documentación que manejen y que utilicen para su realización es responsabilidad suya y los ficheros manuales estructurados o informatizados que necesiten crear con esta finalidad serán propios de su competencia y de su responsabilidad.
Cuestión distinta será la forma de su declaración, en la que habrá que acudir a lo previsto en el artículo 4 de la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid y en el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro de Ficheros de Datos Personales. Atendiendo a esta normativa y siguiendo el procedimiento de declaración previsto, será a través de una Orden del Consejero de Educación como se deberán aprobar los ficheros necesarios para el desarrollo de la actividad de los equipos.
Cuestión distinta será también, el sistema o la aplicación informática que se utilice para el desarrollo automatizado del propio fichero que podrá ser el SICE o cualquier otro homologado en la Comunidad de Madrid, pero sobre el que la APDCM no tiene competencia para pronunciarse.
Por lo que se refiere al "principio de calidad" hay que señalar que la finalidad legítima con la que nos encontramos en este campo, y que justificaría el tratamiento, es la de evitar la discriminación de los niños en función de sus limitaciones, bien por padecer discapacidades físicas, psíquicas, sensoriales, o por manifestar graves trastornos de personalidad o conducta, y conseguir su integración en el sistema educativo, garantizándoles el cumplimiento de los objetivos generales, teniendo los equipos de orientación educativa y psicopedagógica la competencia legal para su desarrollo.
El conjunto de información y documentación, en el que se contienen evidentemente datos de carácter personal y del que es necesario disponer con el objeto de fijar las adaptaciones precisas para que estos menores no sean discriminados, viene determinado por la normativa vigente que regula el procedimiento para la realización de la evaluación psicopedagógica y el dictamen de escolarización.
De esta forma se específica que la evaluación psicopedagógica habrá de reunir la información del alumno y su contexto familiar y escolar que resulte relevante para ajustar la respuesta educativa a sus necesidades y así se cita que, del alumno comprenderá las condiciones de discapacidad o sobredotación, historia educativa y escolar, competencia curricular y estilo de aprendizaje; del contexto escolar comprenderá el análisis de las características de la intervención educativa, de las características y relaciones que se establecen en el grupo-clase, así como de la organización de la respuesta educativa; y por último del contexto familiar analizará y recogerá las características de la familia y de su entorno, expectativas de los padres y posibilidades de cooperación en el desarrollo del programa de atención educativa en el seno familiar.
Asimismo se establece que para efectuar la evaluación psicopedagógica, los profesionales utilizarán los instrumentos propios de las disciplinas implicadas que permitan responder a los requerimientos y objetivos. Entre dichos procedimientos estarán la observación de protocolos para la evaluación de las competencias curriculares, los cuestionarios, las pruebas psicopedagógicas, las entrevistas y la revisión de los trabajos escolares, así como -en determinados casos- la evaluación psicopedagógica de carácter individual.

En consecuencia, se puede señalar como conclusión respecto del principio de calidad que, en la evaluación psicopedagógica -siendo el tipo de información que van a poder obtener, utilizar y tratar los equipos de orientación psicopedagógica o los departamentos de orientación muy amplio y variado (datos del alumno, datos del contexto escolar y datos familiares)-, el respeto a este principio se cumplirá siempre que se recabe y trate la información que se detalla en las disposiciones señaladas.

Por último y respecto a quien podrá acceder a la documentación e información que forma parte de la evaluación, se señala que también este aspecto está previsto en la normativa vigente, en la que se establece que la evaluación psicopedagógica constituye una labor interdisciplinar que podrá ser objeto de análisis y valoración conjunta en el seno del equipo o en el departamento de orientación del centro. Por tanto, son los componentes del equipo los que tienen el acceso a esta información.

Siguiendo con el principio de calidad, hay que diferenciar a continuación el conjunto de información y documentación que constituyen la evaluación, de las conclusiones que se recogerán en el informe psicopedagógico y en el dictamen de escolarización, dado que a este informe y dictamen sí van a tener acceso más profesionales del propio centro y de fuera de él.

Las conclusiones de la evaluación psicopedagogía se recogen en un informe que a su vez forma parte del dictamen de escolarización y constituye el documento en el que de forma clara y completa se reflejará la situación evolutiva y educativa actual de los alumnos de los diferentes contextos y en el que se recogen aspectos tales como los datos personales, historia escolar y motivo de la evaluación; desarrollo general del alumno, que incluirá, en su caso, las condiciones personales de salud, de discapacidad o de sobredotación, el nivel de competencia curricular y el estilo de aprendizaje; aspectos más relevantes del proceso de enseñanza y aprendizaje en el aula y en el centro escolar; influencia de la familia y del contexto social en el desarrollo del alumno; identificación de las necesidades educativas especiales que ha de permitir la adecuación de la oferta educativa, así como la previsión de los apoyos personales y materiales a partir de los recursos existentes o que razonablemente puedan ser incorporados; y las orientaciones para la propuesta curricular.

Por tanto, en el informe no se recogerá toda la información y documentación recabada en el proceso de evaluación, sino aquella que viene específicamente señalada en la normativa aplicable y ello porque tanto al informe como al dictamen de escolarización van a tener acceso terceros distintos de los profesionales que integran los equipos, como serán los profesionales del centro en la medida en que el informe y el dictamen se van a incorporar a los expedientes académicos de los alumnos. A su vez, dentro del proceso de escolarización, van a ser conocidos por la inspección educativa, el Director provincial (Director del Área Territorial) y por la Comisión de Escolarización que corresponda.

De otra parte, en relación con el cumplimiento del principio del consentimiento para poder proceder al tratamiento de la información y documentación recogida en la evaluación psicopedagógica, conviene recordar previamente que, en el ejercicio de esta actividad, se está trabajando con situaciones de incapacidad de menores y que por lo tanto ellos -generalmente- no pueden prestar el consentimiento sino que, de conformidad con el Código Civil (art. 154 y 267) serán sus padres o tutores los que ostentan su representación y los que por tanto deberán expresar su voluntad en este sentido.

Asimismo, debe tenerse en consideración que en determinadas ocasiones entre la información y documentación que se incorpore a la evaluación psicopedagógica pueden existir datos de salud de estos menores (informes médicos, información facilitada por los padres o tutores que haga referencia a la salud de los menores, etc.). En estos casos estos datos determinan una especial protección y refuerzan la forma del consentimiento. Así la LOPD establece en su artículo 7.3 que los datos de carácter

personal que hagan referencia al origen racial, a la salud y a la vida sexual solo podrán ser recabados tratados y cedidos cuando por razones de interés general así lo disponga una ley o el afectado consienta expresamente. En el caso de los equipos de orientación será necesario que dispongan siempre del consentimiento expreso de los padres o tutores para tratar datos de salud de los menores de catorce años (o del propio menor, si es mayor de catorce años), dado que no existe ninguna ley que les habilite el tratamiento sin dicho consentimiento.
Finalmente, en los casos de padres separados, es la resolución judicial la que establece todo lo relativo a la patria potestad y a la guardia y custodia de los hijos, siendo ejercida la primera normalmente por aquel con quien el hijo conviva, salvo que el juez haya determinado que la patria potestad es compartida por ambos progenitores (Art. 156 del Código Civil).
Como señala el artículo 162 del Código Civil, los padres que ostenten la patria potestad tienen la representación legal de sus hijos menores no emancipados. El ejercicio de la patria potestad es determinante para ostentar el ejercicio de la representación legal de los menores y por tanto, para dar el consentimiento y acceder a todos los datos relativos al menor. A estos efectos con la presentación del documento judicial que haga mención a la patria potestad y asignación de guarda y custodia deberá ser suficiente para acceder a la información de los menores.
La comunicación a los padres de los datos relativos a la información de sus hijos no puede considerarse cesión de datos del menor, siempre que ostenten la patria potestad y por tanto su representación legal, sino que es una manifestación del ejercicio del derecho de acceso a datos personales por parte de los representantes legales del afectado.
Desde el punto de vista de la legislación de protección de datos, no existe ningún motivo que impida a un padre separado la solicitud de información de su hijo, siempre que ostente la patria potestad, condición que podrá acreditarse con la presentación del documento judicial que regule esta materia.

¿Resultaría conforme con la LOPD que se comunicase por el Centro de Educación de Personas Adultas de una Mancomunidad a un Ayuntamiento la identificación de un alumno, menor de edad, causante de un determinado deterioro en el mobiliario de las aulas de un Centro educativo cuya titularidad pertenece a dicho Ayuntamiento?

La comunicación de los datos a los que se refiere la consulta constituye una auténtica cesión de datos, definida por el artículo 3 i) de la LOPD como "Toda revelación de datos realizada a una persona distinta del interesado".
Con carácter general, la comunicación de datos personales quedará sometida a lo dispuesto por el artículo 11.1 de la citada Ley Orgánica, en cuya virtud "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"; esta disposición se ve excepcionada, entre otros supuestos, por lo dispuesto en el apartado 2.a) del propio artículo 11 de la meritada Ley Orgánica, que posibilita la cesión inconsentida de los datos en caso de que la misma se encuentre fundamentada en lo establecido por una norma con rango de Ley.
De manera concreta, el artículo 1089 del Código Civil dispone que "Las obligaciones nacen de la ley, de los contratos, y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia". A su vez, debe señalarse que en cuanto al posible surgimiento de una responsabilidad extracontractual, posiblemente perseguida por el Ayuntamiento que solicita la comunicación de los datos identificativos del alumno y, en su caso, invocable ante los Tribunales, el artículo 1902 del Código Civil dispone que "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".

El requisito principal exigido por la Jurisprudencia para la aplicación de este precepto es la existencia de una relación causal directa entre el acto u omisión del agente y el daño causado en los derechos de la personalidad o en el patrimonio del perjudicado. Pues bien, como parece deducirse del contenido del escrito de consulta, resultaría evidente la existencia de una relación causal entre la actividad del alumno causante del daño y el daño causado, siendo así que el perjuicio sería realmente ocasionado por una actuación negligente o simplemente dañosa del alumno menor de edad.
En consecuencia, producido el perjuicio al Ayuntamiento interesado, en su caso, los órganos jurisdiccionales podrían exigir la correspondiente indemnización mediante la aplicación de los principios de la responsabilidad extracontractual, al quedar determinada la existencia de la relación de causalidad exigible por el artículo 1902 del Código Civil, en cuya virtud "el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado", pudiendo exigirse del culpable la restitución del daño emergente y del lucro cesante.
A ello no podrán oponerse las previsiones del artículo 9 ("Seguridad de los datos") de la LOPD, ni lo dispuesto por su artículo 10 ("Deber de secreto"), por cuanto aún adoptando el Responsable del fichero las medidas de seguridad legalmente exigibles a fin de evitar que pueda producirse una vulneración del deber de secreto, ello no impide que el centro consultante deba subvenir a la petición cursada por el titular de las instalaciones en las que se presta su actividad docente, en aras de la exigencia de las acciones que en derecho le corresponden, tales como exigir judicialmente del causante del daño (o, en el presente supuesto, de sus padres, tutores o representantes legales) la correspondiente indemnización por los daños y perjuicios causados, en aplicación del principio contenido en el transcrito artículo 1902 del Código Civil.
Así, con base en lo dispuesto por los citados preceptos legales, el centro educativo podría proceder a la cesión de los datos de carácter personal identificativos del menor que ha ocasionado el deterioro en las aulas del edificio (centro educativo), propiedad del Ayuntamiento, en el que se imparte enseñanza por el centro consultante. En conclusión, sin necesidad de que concurra el consentimiento del afectado (ni de sus padres, tutores o representantes legales), el centro educativo consultante podrá ceder al Ayuntamiento solicitante los referidos datos de carácter personal.
En relación con la posible existencia de otras habilitaciones legales específicas que, basadas en normas con rango de ley formal, amparen la cesión inconsentida del tipo de datos al que se refiere la consulta, conviene traer a colación lo previsto por el artículo 8 ("Cooperación entre Administraciones") de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, de acuerdo con el cual:
"Artículo 8.Cooperación entre Administraciones.
1. Las Administraciones educativas y las Corporaciones locales coordinarán sus actuaciones, cada una en el ámbito de sus competencias, para lograr una mayor eficacia de los recursos destinados a la educación y contribuir a los fines establecidos en esta Ley.
2. Las ofertas educativas dirigidas a personas en edad de escolarización obligatoria que realicen las Administraciones u otras instituciones públicas, así como las actuaciones que tuvieran finalidades educativas o consecuencias en la educación de los niños y jóvenes, deberán hacerse en coordinación con la Administración educativa correspondiente".
De otra parte, debe señalarse lo dispuesto por los artículos 72, 81, 112, de la citada Ley Orgánica 2/2006, de 3 de mayo, de Educación, según los cuales:
"Artículo 72.Recursos.
1. Para alcanzar los fines señalados en el artículo anterior, las Administraciones educativas dispondrán del profesorado de las especialidades correspondientes y de

profesionales cualificados, así como de los medios y materiales precisos para la adecuada atención a este alumnado.
2. Corresponde a las Administraciones educativas dotar a los centros de los recursos necesarios para atender adecuadamente a este alumnado. Los criterios para determinar estas dotaciones serán los mismos para los centros públicos y privados concertados.
(…)
5. Las Administraciones educativas podrán colaborar con otras Administraciones o entidades públicas o privadas sin ánimo de lucro, instituciones o asociaciones, para facilitar la escolarización y una mejor incorporación de este alumnado al centro educativo".
"Artículo 81.Escolarización.
(…)
4. Sin perjuicio de lo dispuesto en el capítulo I de este mismo título, las Administraciones educativas dotarán a los centros públicos y privados concertados de los recursos humanos y materiales necesarios para compensar la situación de los alumnos que tengan especiales dificultades para alcanzar los objetivos de la educación obligatoria, debido a sus condiciones sociales".
"Artículo 112.Medios materiales y humanos.
1. Corresponde a las Administraciones educativas dotar a los centros públicos de los medios materiales y humanos necesarios para ofrecer una educación de calidad y garantizar la igualdad de oportunidades en la educación.
2. En el contexto de lo dispuesto en el apartado anterior, los centros dispondrán de la infraestructura informática necesaria para garantizar la incorporación de las tecnologías de la información y la comunicación en los procesos educativos. Corresponde a las Administraciones educativas proporcionar servicios educativos externos y facilitar la relación de los centros públicos con su entorno y la utilización por parte del centro de los recursos próximos, tanto propios como de otras Administraciones públicas.
3. Los centros que escolaricen alumnado con necesidad específica de apoyo educativo, en proporción mayor a la establecida con carácter general o para la zona en la que se ubiquen, recibirán los recursos complementarios necesarios para atender adecuadamente a este alumnado.
4. Las Administraciones educativas facilitarán que aquellos centros que, por su número de unidades, no puedan disponer de los especialistas a los que se refiere el artículo 93 de esta Ley, reciban los apoyos necesarios para asegurar la calidad de las correspondientes enseñanzas.
5. Las Administraciones educativas potenciarán que los centros públicos puedan ofrecer actividades y servicios complementarios a fin de favorecer que amplíen su oferta educativa para atender las nuevas demandas sociales, así como que puedan disponer de los medios adecuados, particularmente de aquellos centros que atiendan a una elevada población de alumnos con necesidad específica de apoyo educativo".
De otra parte, la Disposición Adicional Decimoquinta ("Municipios, corporaciones o entidades locales") de la citada Ley Orgánica de Educación, prevé que:
"1. Las Administraciones educativas podrán establecer procedimientos e instrumentos para favorecer y estimular la gestión conjunta con las Administraciones locales y la colaboración entre centros educativos y Administraciones públicas.
En lo que se refiere a las corporaciones locales, se establecerán procedimientos de consulta y colaboración con sus federaciones o agrupaciones más representativas.
2. La conservación, el mantenimiento y la vigilancia de los edificios destinados a centros públicos de educación infantil, de educación primaria o de educación especial, corresponderán al municipio respectivo. Dichos edificios no podrán destinarse a otros

servicios o finalidades sin autorización previa de la Administración educativa correspondiente.
(…)".
En conclusión, de la normativa citada se extrae claramente la existencia de habilitaciones legales suficientes, basadas en normas con rango de ley formal, en orden a la comunicación de los datos de carácter personal objeto de la pregunta.
A nuestro juicio, todo lo anterior no entra en contradicción con las funciones propias de la “inspección del sistema educativo”, regulada en los artículos 148 y siguiente de la Ley Orgánica 2/2006, de 3 de mayo, en cuya virtud:
"Artículo 148.Inspección del sistema educativo.
1. Es competencia y responsabilidad de los poderes públicos la inspección del sistema educativo.
2. Corresponde a las Administraciones públicas competentes ordenar, regular y ejercer la inspección educativa dentro del respectivo ámbito territorial.
3. La inspección educativa se realizará sobre todos los elementos y aspectos del sistema educativo, a fin de asegurar el cumplimiento de las leyes, la garantía de los derechos y la observancia de los deberes de cuantos participan en los procesos de enseñanza y aprendizaje, la mejora del sistema educativo y la calidad y equidad de la enseñanza".
Finalmente, en relación con la comunicación de los datos personales de los alumnos (también en el supuesto de los menores de edad), es menester referir lo dispuesto por la Disposición Adicional Vigésimo Tercera ("Datos personales de los alumnos") de la tan citada Ley Orgánica 2/2006, de 3 de mayo, de Educación, y especialmente lo establecido en su Apartado 4:
"1. Los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de su función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos.
2. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos. En todo caso, la información a la que se refiere este apartado será la estrictamente necesaria para la función docente y orientadora, no pudiendo tratarse con fines diferentes del educativo sin consentimiento expreso.
3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad. El profesorado y el resto del personal que, en el ejercicio de sus funciones, acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.
4. La cesión de los datos, incluidos los de carácter reservado, necesarios para el sistema educativo, se realizará preferentemente por vía telemática y estará sujeta a la legislación en materia de protección de datos de carácter personal, y las condiciones mínimas serán acordadas por el Gobierno con las Comunidades Autónomas en el seno de la Conferencia Sectorial de Educación".
A su vez, el Centro educativo consultante deberá estar a lo dispuesto por el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, en relación con el denominado "principio de calidad de los datos", de acuerdo con el cual "1. Los datos de carácter persona sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el

ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. 2 Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".
De acuerdo con lo anterior, la comunicación de los datos identificativos del alumno del centro, menor de edad, al Ayuntamiento solicitante de dicha información, deberá resultar adecuada, pertinente y no excesiva en relación con la finalidad prevista, relativa a la mera identificación del menor afectado.
En conclusión, de conformidad con el artículo 4 de la LOPD, los datos que se faciliten del menor al Ayuntamiento solicitante deberán ser adecuados, pertinentes y no excesivos para la finalidad para la cual se recaban, debiendo ser cancelados o borrados cuando hayan dejado de ser necesarios para la finalidad que motivó dicha recogida.
Asimismo, tal y como se ha adelantado, tanto por parte del cedente de la información como por el cesionario de la misma, deberá garantizarse que, de acuerdo con lo dispuesto por el artículo 10 de la LOPD, y en el artículo 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, quede debidamente asegurado el deber de secreto de todas las personas que conozcan la información de carácter personal relativa al alumno al que se refiere la solicitud objeto de la pregunta.

¿Es necesaria la autorización del afectado o de su representante legal para el intercambio de fotografías de los alumnos en un determinado proyecto educativo? ¿Y para publicar fotografías e imágenes de los estudiantes en Internet?

De acuerdo con lo dispuesto por la LOPD y por su normativa de desarrollo, las fotografías de las personas físicas identificadas o identificables deben ser consideradas como datos de carácter personal. Así, con carácter general, puede señalarse que los datos de carácter personal, se definen en el artículo 3 a) de la citada Ley Orgánica como "cualquier información concerniente a personas físicas identificadas o identificables".
Con base en la definición anterior será suficiente con que los datos permitan la identificación de una persona concreta para que se trate de datos de carácter personal.
A su vez, el artículo 5.1 f) del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD, considera datos de carácter personal a "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".
En atención a las citadas definiciones legales, las imágenes deben ser consideradas datos de carácter personal, dado que las mismas permiten la identificación de las personas que aparecen en dichas imágenes, rigiéndose por tanto por lo dispuesto en la LOPD.
Según prevé el artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. Asimismo, en su artículo 11.1 establece que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Así pues, con carácter general, para el tratamiento y cesión de los datos de carácter personal se requiere que los afectados por dichos tratamientos así lo consientan.
El envío de fotografías o filmaciones de actividades escolares para la difusión e intercambio de experiencias en el ámbito educativo entre los miembros de un

determinado Proyecto, constituye una cesión de datos, definida por el artículo 3 i) de la LOPD como "toda revelación de datos realizada a una persona distinta del interesado".
A su vez, la publicación de fotografías e imágenes de estudiantes a través de Internet debe reputarse -asimismo- comunicación o cesión de datos. En dicho supuesto, además, dicha cesión se realiza de forma indiscriminada, dado que cualquier persona que acceda a la página Web puede recabar la correspondiente información sin necesidad de ostentar ningún interés legítimo y determinado.
De tal suerte, dicha captación y cesión de datos requiere que la comunicación se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y el cesionario y que el interesado preste su consentimiento, según prevé el artículo 11.1 de la LOPD, salvo que concurra alguna de las excepciones previstas en el apartado 2, que en el presente caso no se presentan.
Sin embargo, del tenor literal de la documentación que se acompaña a la consulta ("solicitud de autorización en relación con el envío de fotografías de los alumnos en el ámbito de un determinado proyecto educativo" y "modelo de permiso para publicar fotos e imágenes de los estudiantes en Internet"), se desprende que para la cesión de las fotografías y filmaciones en el marco del Proyecto educativo, así como para la publicación de las mismas en Internet, se obtendrá previamente el consentimiento del padre/madre/tutor de los menores afectados, a través de la correspondiente autorización escrita cuya copia se acompaña.
En consecuencia, podría concluirse que, al cumplir con la exigencia del consentimiento previsto en los artículos 6 y 11 de la LOPD, el tratamiento y cesión de los datos personales a los que se refiere la pregunta resultaría conforme con lo dispuesto por dicha Ley Orgánica.
Sin embargo, precisando lo anterior, debe señalarse que -con carácter general- siempre que se soliciten datos de carácter personal, la LOPD obliga en su artículo 5 a que previamente se informe:
"a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".
Igualmente señala dicho artículo que cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior, no siendo necesaria la información a que se refieren las letras b), c) y d) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban, debiéndose informar, en cualquier caso, de la existencia del fichero, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección del responsable del fichero.
Tal como queda expuesto, del contenido de las "autorizaciones y permisos" objeto de esta pregunta, se deduce que el centro educativo consultante procederá al tratamiento de datos de carácter personal. En consecuencia, para el supuesto de que los referidos tratamientos no hayan sido objeto de declaración e inscripción en el Registro de Ficheros de esta Agencia, deberá procederse a la creación, notificación e inscripción del correspondiente fichero con datos de carácter personal, siguiendo el procedimiento previsto en el artículo 4 de la Ley 8/2001, de 13 de julio de Protección de Datos de Carácter Personal en la Comunidad de Madrid y desarrollado posteriormente por el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de

disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro.
En conclusión, dado que de este tipo de actividades derivan cesiones de datos personales, con carácter previo a su realización, se debe informar al interesado sobre el tratamiento de datos previsto y sobre las cesiones de datos que se pretenden realizar en los términos previstos en el artículo 5 de la LOPD, y obtener su consentimiento al respecto, debiéndose -a su vez- cumplir con el resto de las obligaciones establecidas por la normativa sobre protección de datos de carácter personal.

¿Es posible el acceso a los datos de alumnos matriculados en el último curso de formación profesional en los centros educativos de la Comunidad de Madrid por parte de una empresa privada para llevar a cabo un estudio estadístico sobre formación profesional para el Consejo Superior de Cámaras?

La LOPD establece que para proceder a la cesión de los datos de carácter personal se precisará el consentimiento de los afectados. Sin embargo, esta norma general de consentimiento no es absoluta, y la propia ley recoge una serie de excepciones, entre las que se encuentra la posibilidad de que la cesión se produzca entre dos Administraciones Públicas, plasmada en su artículo 21. Esta cesión entre Administraciones Públicas no tendrá lugar cuando se lleve a cabo para el ejercicio de competencias diferentes o que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
Teniendo en cuenta que la cesión de datos se produciría entre dos Administraciones Públicas, ya que los ficheros corresponden a los Centros Educativos de Formación Profesional dependientes de la Consejería de Educación de la Comunidad de Madrid, y que se cederían al Consejo Superior de Cámaras para el cumplimiento de una función público-administrativa que se concreta en la elaboración de un estudio sobre la inserción laboral de los titulados de formación profesional de los últimos años, sería de aplicación la referida excepción del artículo 21 de la LOPD, y de esta manera, los datos de los alumnos matriculados en el tercer curso de formación profesional en cada uno de los centros educativos que imparten esta formación en la Comunidad de Madrid podrían ser cedidos al Consejo Superior de Cámaras sin el consentimiento de cada uno de los afectados.
No obstante, a los efectos de que la cesión de datos pudiera tener el amparo legal previsto en el artículo 21 LOPD, sería necesario que por parte del Consejo Superior de Cámaras se establecieran una serie de garantías que el ordenamiento jurídico ha previsto.
En este sentido, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común fija en su artículo 2 el ámbito de aplicación de la misma, señalando que tienen la consideración de Administraciones Publicas, la Administración General del Estado; las Administraciones de las Comunidades Autónomas; las Entidades que integran la Administración Local y finalmente las Entidades de Derecho Público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las Administraciones Públicas. Igualmente y con base en la disposición transitoria primera de dicha Ley, las Corporaciones de Derecho Público quedan encuadradas en su ámbito de aplicación y tendrán por tanto la consideración de Administración Publica formando lo que se denomina doctrinalmente la Administración Corporativa, siempre que ejerzan potestades administrativas.
El artículo 1.1 de la Ley 3/1993, de 22 de marzo, Básica de las Cámaras Oficiales de Comercio, Industria y Navegación, establece que: "Las Cámaras Oficiales de

Comercio, Industria y, en su caso, de Navegación son Corporaciones de derecho público con personalidad jurídica y plena capacidad de obrar para el cumplimiento de sus fines, que se configuran como órganos consultivos y de colaboración con las Administraciones Públicas, sin menoscabo de los intereses privados que persiguen".
Dentro de las funciones desarrolladas por las referidas Cámaras, pueden distinguirse aquéllas que persiguen un interés privado de sus miembros (las personas naturales o jurídicas que ejerzan actividades comerciales, industriales y navieras), de aquéllas otras que suponen el ejercicio de auténticas potestades administrativas, vinculadas al ejercicio por la corporación de potestades publicas y en consecuencia sujetas al régimen jurídico de las Administraciones Públicas, de conformidad con la disposición transitoria primera de la Ley 30/1992, de 26 de noviembre.
Las funciones publico-administrativas que pueden ejercer las Cámaras Oficiales de Comercio, Navegación e Industria, vienen definidas en el artículo 2 de la Ley 3/1993, de 22 de marzo, en cuyo apartado 2.a) establece que les corresponde elaborar estadísticas del comercio, la industria y la navegación y realizar las encuestas de evaluación y los estudios necesarios que permitan conocer la situación de los distintos sectores, con sujeción, en todo caso, a lo dispuesto en la Ley sobre Función Estadística Pública y demás disposiciones aplicables.
Por otra parte en el artículo 18 de la Ley, en el que se regula el Consejo Superior de Cámaras, se establece que es una Corporación de Derecho Público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines y está integrado por representantes de la totalidad de las correspondientes Cámaras Oficiales de Comercio, Industria y Navegación.
En conclusión, en relación con la pregunta planteada, en primer lugar se debería garantizar que la empresa que va a realizar el sondeo por cuenta del Consejo Superior de Cámaras haya suscrito el oportuno contrato de tratamiento de datos personales, atendiendo a lo dispuesto en el artículo 12 de la LOPD.
Igualmente se debería garantizar que la estudio se va a realizar de conformidad con las previsiones contenidas en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, ajustando la recogida de datos a los principios de secreto, transparencia, especialidad y proporcionalidad.
Asimismo, si la empresa privada va a recoger datos de carácter personal a la hora de contactar con los alumnos para realizar las preguntas objeto de la encuesta, tendrá que cumplir con el derecho de información en la recogida de datos regulado en el artículo 5 de la LOPD.

¿Un Colegio Profesional puede tener acceso anual al listado de alumnos aprobados en el último curso del centro de estudio de la profesión en cuestión para enviarles información colegial necesaria para que puedan incorporarse al mundo laboral de ese sector?

No, a pesar de los fines esenciales de los colegios profesionales de ordenar el ejercicio de la profesión y adoptar las medidas necesarias para evitar el intrusismo profesional y la competencia desleal.
Esto es así porque dichos fines no ampararían el posible acceso de un colegio profesional a un listado de alumnos que están cursando los estudios de la profesión pero que todavía no han empezado a ejercer la profesión en cuestión y de los que no se sabe cuántos de ellos finalmente ejercerían dicha profesión. Por lo cual, para poder acceder a esta información regiría el principio general del artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siendo necesario contar con el consentimiento de cada alumno.
Una solución alternativa, que encajaría con la función de informar de la necesidad de la colegiación para el ejercicio de la profesión en cuestión y que cumpliría con la LOPD,

sería que el Colegio Profesional enviase la información al Centro donde se cursan los estudios para que a través de ella se informe a los alumnos del último curso de la carrera.

Cesiones de datos del personal de los Centros Educativos

¿Qué datos de los empleados públicos se pueden facilitar a los Delegados de Prevención del Comité de Seguridad y Salud de un Centro Educativo con el objeto de que se puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores para valorar sus causas y proponer las medidas oportunas?

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales establece como competencia del Comité de Seguridad y Salud conocer y analizar los daños producidos en la salud o en la integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas (artículo 39.2.c).
Por lo tanto, puede tener acceso, sin contar con el consentimiento del afectado al concurrir la excepción de que una norma con rango de ley prevea la cesión, a un listado en que se incluya nombre y apellidos de los trabajadores accidentados, fecha del accidente, fechas de alta y baja, tipo de lesión/región anatómica y forma en que se produjo o agente que causó dicho accidente, siempre y cuando dicho conocimiento tengan como finalidad conocer y analizar los daños producidos en la salud o integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas.

El Comité de empresa o el Delegado de personal de un Centro Educativo han solicitado un listado nominativo de todos los empleados. ¿Cuáles son los datos que pueden entregarse a los representantes sindicales?

Los datos que se deben facilitar al Comité de Empresa o a los Delegados de Personal se encuentran regulados en el artículo 64 del Estatuto de los Trabajadores, en su número 1, en el que se indica que el Comité de Empresa tiene, dentro de sus competencias, las de recibir información del empresario sobre ciertos aspectos. El Comité de Empresa ejerce unas funciones de vigilancia y protección, sin necesidad de acceder a información diferente de la que marque la Ley.
A la vista de las previsiones legales que habilitan las funciones y competencias de las Secciones Sindicales, Comités de Empresa y Juntas de Personal, se considera que, de acuerdo con la LOPD, dichas previsiones no especifican con carácter general que se tenga que proceder a la cesión de datos personales de los empleados públicos en los siguientes supuestos: para conocer el establecimiento de la jornada laboral y horario de trabajo, régimen de permisos, vacaciones y licencias; emitir informe sobre materias como traslado total o parcial de las instalaciones, planes de formación de personal o implantación o revisión de sistemas de organización y método de trabajo; conocer las estadísticas sobre el índice de absentismo y sus causas, los accidentes en acto de servicio y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del ambiente y las condiciones de trabajo, así como las correspondientes a recibir información trimestral sobre política de personal.
Por tanto, con carácter general, estas funciones quedarán plenamente cumplidas por parte de los centros educativos públicos mediante la cesión a las Secciones Sindicales, los Comités de Empresa, Juntas y/o Delegados de Personal, de la información debidamente disociada, según el procedimiento definido en el artículo 3 f) de la LOPD,

que permita a aquéllos conocer las circunstancias relativas a la política de personal sin referenciar la información en un sujeto concreto.
No obstante lo anterior y en el supuesto en que un empleado público haya planteado una queja ante su Sección sindical, Comité, Junta o Delegado de Personal correspondiente, relativa a sus condiciones de trabajo, será posible la cesión del dato específico de dicha persona.
Sin embargo, debe tenerse en cuenta que el legislador puede prever específicamente aquellos datos de carácter personal de los trabajadores que pueden ser cedidos a las Secciones Sindicales, Comités de Empresa, Juntas y Delegados de Personal, y de esa forma, la necesidad del consentimiento de los afectados quedaría excepcionada. Por otro lado, no hay que olvidar la función de la Jurisprudencia constitucional y ordinaria en la interpretación tanto del derecho a la libertad sindical como del derecho fundamental a la protección de datos personales.
Entre los supuestos legales que contemplan las cesiones de datos, se podrían señalar, entre otros, los siguientes:
1. Será posible la cesión de los datos que figuren en la copia básica de los contratos de trabajo -artículos 64 y 8.3 del Estatuto de los Trabajadores-, dado que específicamente figura como información concreta a facilitar a los representantes de los trabajadores, con la excepción del DNI, el domicilio del trabajador, estado civil y cualquier otro dato que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo afecte a la intimidad personal de los empleados.
2. Igualmente, será posible la cesión en el caso de obtener información de las sanciones impuestas por faltas muy graves a los trabajadores -artículo 64 E.T. y artículo 9 de la Ley 9/1987-.
3. Por otra parte, en el caso del personal funcionario y respecto del complemento de productividad, el artículo 23.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, tras definir en su apartado c) el citado complemento, indica, en el último párrafo de este apartado, que "en todo caso, las cantidades que perciba cada funcionario por este concepto serán de conocimiento público de los demás funcionarios del Departamento u Organismo interesado así como de los representantes sindicales".
4. Asimismo en el caso de vigilancia de la salud, los artículos 36.2 b) y 39.2 c) de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, habilitan a que los Delegados de Prevención que forman parte del Comité de Seguridad e Higiene puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas. En consecuencia y con las limitaciones previstas en el artículo 22.4 del mismo texto legal podrán tener acceso, por ejemplo, al nombre y apellidos de los trabajadores, fecha del reconocimiento médico, fechas de alta y baja y conclusiones del reconocimiento médico.
5. Igualmente el artículo 11.2 de la Ley Orgánica de Libertad Sindical prevé que el empresario proceda al descuento de la cuota sindical sobre los salarios de los trabajadores afiliados y su transferencia al sindicato correspondiente, siempre que exista conformidad del trabajador. Es decir, aquí se trata de un supuesto de cesión de datos habilitados por ley (transferencia de la cuota sindical), pero que necesita del consentimiento del trabajador afectado, dado que el trabajador, para cumplir con su obligación del pago de la cuota, puede optar por su abono directo al sindicato sin necesidad de que la empresa se lo descuente de la nómina.
6. Por último y a los efectos de informar a todos los empleados públicos pertenecientes a cada uno de los ámbitos de negociación, de conformidad con el artículo 64.12 del Estatuto de los Trabajadores y el artículo 9.10 de la Ley 9/1987, de 12 de junio, y siguiendo la doctrina del Tribunal Constitucional (ver por ejemplo STC 142/1993, STC 213/2002 y la más reciente STC 281/2005) se entiende que podrían

tener acceso al nombre, apellidos y la dependencia administrativa donde prestan sus servicios cada uno de dichos empleados públicos, así como a la dirección de correo electrónico en el supuesto de que la Unidad administrativa se la haya asignado.
En este último supuesto referido a facilitar la dirección de correo electrónico de los empleados a los representantes sindicales, hay que resaltar la importancia del uso al que puede ser destinado por estos y que viene reconocido en la propia sentencia 281/2005 del Tribunal Constitucional. Así, se señala que el derecho a enviar información sindical tanto a los afiliados como a los no afiliados forma parte del derecho de libertad sindical (FJ4), si bien está sujeto a límites o restricciones, como son las referidas a que sólo se justifica su uso para transmitir información de naturaleza sindical y laboral …. Y que la comunicación no puede perturbar la actividad normal de la empresa (FJ8). En este sentido, señala el TC que resultaría constitucionalmente lícito que la empresa predeterminase las condiciones de utilización para fines sindicales de las comunicaciones electrónicas siempre que no las excluyera en términos absolutos (FJ8).
Por último, hay que señalar que de conformidad con el derecho de oposición reconocido en el artículo 6.4 LOPD, los empleados públicos que no quieran recibir información sindical pueden oponerse a este tratamiento, y la representación sindical como responsable del envío tendrá la obligación de dejar de enviar información a todos aquellos que hayan ejercitado este derecho.

¿Pueden los representantes sindicales solicitar datos de los profesores en relación con el horario de los mismos? ¿Y sobre los datos relativos a profesores afectados por absentismo laboral?

Las funciones de vigilancia y protección del Comité de Empresa enumeradas en el artículo 64 del Estatuto de los Trabajadores, así como las correspondientes a recibir información trimestral sobre política de personal, no determinan específicamente la cesión de datos de carácter personal, circunstancia esta determinante para poder facilitar esta información de acuerdo con la LOPD.
En consecuencia estas funciones tienen que desarrollarse sin necesidad de proceder a una cesión masiva de los datos personales referentes al personal que presta sus servicios en los diferentes centros educativos públicos, salvo que hubieran dado su consentimiento, y ello derivado de que, con carácter general, dicha cesión de datos no está contemplada específicamente ni en el Estatuto de los Trabajadores, ni en la Ley 9/1987, de 12 de junio, de Órganos de Representación, determinación de las condiciones de trabajo y participación del personal al servicio de las Administraciones Públicas.
Por el contrario, con carácter general las funciones de control y de información quedarán plenamente satisfechas mediante la cesión, tanto a los Comités de Empresa como a las Juntas, Delegados de Personal y Secciones Sindicales, de la información debidamente disociada según el procedimiento definido en el artículo 3 f) de la LOPD, que permita a aquéllos conocer las circunstancias relativas a la política de personal, sin referenciar la información a un sujeto concreto.
Asimismo, se podrá proporcionar la información de las horas extraordinarias y el motivo de su realización sin asociarse a la identidad de los trabajadores que las hayan realizado, a no ser que éstos hubiesen manifestado previamente su consentimiento. De la misma manera se puede proporcionar el dato del absentismo laboral registrado, sin comunicación de los trabajadores afectados.
¿Pueden ser cedidos por parte de la Dirección General de Recursos Humanos de la Consejería de Educación los datos referentes al número de puestos de trabajo, las titulaciones y nivel de estudios realizados, edades y adaptación de funciones

de puestos de trabajadores con número de puesto de trabajo de las categorías a extinguir del personal laboral a una organización sindical?

Se ha de tener en cuenta que la información a la que se refiere esta pregunta corresponde a personal laboral de la Comunidad de Madrid. Atendiendo a lo establecido en el artículo 8.3 a) del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el Texto Refundido del Estatuto de los Trabajadores, con el fin de comprobar la adecuación del contenido del contrato a la legalidad vigente, el empresario entregará a la representación legal de los trabajadores una copia básica de los contratos que se hayan de efectuar por escrito. En esta copia básica figurarán la totalidad de los datos del contrato a excepción del documento nacional de identidad, domicilio, estado civil, y cualquier otro que, de acuerdo con la legislación en materia de protección de datos, se considere que pueda afectar a la intimidad personal.
Las titulaciones y el nivel de estudios realizados son elementos contenidos en el contrato de trabajo y que por lo tanto podrán se conocidos por los representantes legales de los trabajadores que, como establece el Estatuto de los Trabajadores, son los Delegados de Personal y el Comité de Empresa, a través de la copia básica del contrato que la Dirección General de Recursos Humanos de la Consejería de Educación les entrega, pero no por el sindicato correspondiente.
En cuanto a la edad de los trabajadores, hay que señalar que se trata de un dato de carácter personal que, salvo que medie consentimiento expreso del afectado, no podrá ser conocido por los representantes legales de los trabajadores, y por consiguiente, tampoco por los sindicatos, por lo que debe ser eliminado el campo referente a la fecha de nacimiento de la copia básica.
Los datos referentes a la minusvalía de los trabajadores que permite la adaptación de sus respectivos puestos de trabajo, son datos referentes a la salud, especialmente protegidos según la LOPD, y solo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado lo consienta expresamente, por lo que ni los representantes de los trabajadores ni los sindicatos pueden conocer las minusvalías que obligan a adaptar el puesto de trabajo a las funciones que pueda realizar el trabajador afectado.
Los datos correspondientes al número de puesto de trabajo de las categorías a extinguir pueden ser conocidos por los miembros del Comité de Empresa y Delegados de Personal, puesto que, según recoge el artículo 64.4 del Estatuto del los Trabajadores, el Comité de Empresa y los Delegados de Personal deberán tener conocimiento de todas las medidas que puedan suponer una reestructuración de la plantilla para poder realizar un informe previo a las mismas.
En cuanto a las relaciones de puestos de trabajo hay que señalar que de conformidad con el artículo 15.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, se establece el carácter público de dichas relaciones, si bien, las mismas, no contendrán, a la vista del contenido exigido por el artículo 15.1 b), los datos personales del funcionario concreto que ocupe un determinado puesto de trabajo, sino exclusivamente las características de cada uno de los puestos de trabajo existentes en cada dependencia administrativa.

¿Es conforme con la normativa sobre protección de datos la entrega al Comité de Empresa de Centros Educativos de la Relación de Puestos de Trabajo de dichos Centros, con detalle del centro de trabajo, nombre de los trabajadores de cada centro, categoría profesional de los trabajadores, número de puesto que cada uno ocupa, turno y horario de cada uno, tipo de contrato de cada trabajador, antigüedad y número de vacantes de cada centro?
El artículo 64.1.9º del Estatuto de los Trabajadores dispone que el Comité de Empresa ejercerá, entre otras competencias, una labor de vigilancia en el cumplimiento de las

normas vigentes en materia laboral, de seguridad social y empleo. Esta facultad de vigilancia de los Comités de Empresa se ve desarrollada específicamente en el ámbito de la Comunidad de Madrid, a través del vigente Convenio Colectivo del Personal Laboral de la Comunidad de Madrid, en donde se acuerda que los representantes de los Delegados de Personal y Comités de Empresa tendrán derecho a conocer y consultar el registro de accidentes de trabajo y las causas de los mismos, a acceder a los modelos TC1 y TC2 de las cotizaciones a la Seguridad Social, al listado de nómina de cada mes, al calendario laboral, a los presupuestos de los Centros y a un ejemplar de la memoria anual del Centro, así como a cuantos otros documentos relacionados con las condiciones de trabajo afecten a los trabajadores, siempre que, en el caso de acceso a datos personales y para los supuestos así establecidos legalmente, éstos expresen su consentimiento.
En este sentido se considera que, el ejercicio de las competencias y las funciones de vigilancia y protección de las condiciones de trabajo, puede llevarse a cabo sin necesidad de proceder a una cesión masiva de los datos personales referentes al personal y ello derivado de que, con carácter general, dicha cesión de datos no está contemplada específicamente en la Ley. Con carácter general las funciones de control y de información quedarán plenamente satisfechas mediante la cesión a los Comités de Empresa, Juntas, Delegados de Personal y Secciones Sindicales de la información debidamente disociada. Lo anteriormente señalado quedará exceptuado, en el supuesto de que la ley específicamente prevea la entrega de documentos o información que comprenda datos personales de los trabajadores o empleados, como por ejemplo se prevé en el artículo 8.3 del Estatuto de los Trabajadores, al establecer que el empresario entregará a la representación legal de los trabajadores una copia básica de todos los contratos de trabajo que se celebren por escrito.
En cuanto a las Relaciones de Puestos de Trabajo, éstas tienen la finalidad legal de recoger las características individuales de cada uno de los puestos en los que se estructuran las diferentes dependencias administrativas. Su regulación específica se plasma en el artículo 15.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, que establece el carácter público de dichas Relaciones, si bien, las mismas no contendrán los datos personales del funcionario concreto que ocupe un determinado puesto de trabajo, sino exclusivamente las características de cada uno de los puestos de trabajo existentes en cada dependencia administrativa. Esta previsión viene igualmente regulada en la Ley 1/1986, de 10 de abril, de la Función Publica de la Comunidad de Madrid. Hay que señalar que los datos de nombre, apellidos y cargo referidos a cada funcionario público que ocupe cada uno de los puestos de trabajo está restringido a éste último, no pudiendo cederse esa información personal con carácter general sin el consentimiento inequívoco de cada funcionario.
Por lo tanto, se podrá entregar al Comité de Empresa de los Centros Educativos la Relación de Puestos de Trabajo de todos los centros incluidos en el ámbito de actuación del referido Comité, sin que entre los datos que se faciliten conste dato personal alguno, salvo que se haya obtenido previamente el consentimiento del afectado.

¿Se pueden facilitar a las Centrales Sindicales promotoras de las elecciones a la Junta de Personal Docente datos personales de los funcionarios docentes electores, a los efectos de realizar un envío de propaganda electoral?

La comunicación de los datos de carácter personal del personal docente funcionario por parte de Dirección General de Recursos Humanos de la Consejería de Educación a las Centrales Sindicales promotoras de un proceso electoral a la Junta de Personal de centros de enseñanza constituiría una cesión de datos.

Según lo establecido en el artículo 11 de la LOPD, la norma general para llevar a cabo cesiones de datos es contar con el consentimiento de los interesados, debiendo ésta además perseguir un fin legítimo entre cedente y cesionario. No obstante, el propio artículo 11 recoge una serie de excepciones a esta norma general, entre las que se encuentra la posibilidad de que una ley permita la cesión, por lo que habrá que valorar si la comunicación de los datos solicitados por las Centrales Sindicales promotoras de las elecciones tienen o no fundamento legal gozando, si se diera este caso, de la excepcionalidad legal del consentimiento analizada anteriormente.
El artículo 26 de la ley 9/1987, de 12 de junio, de Órganos de Representación, Determinación de las Condiciones de Trabajo y Participación del Personal al Servicio de las Administraciones Públicas, modificado por la Ley 18/1994, de 30 de junio, establece que, cuando se trate de elecciones a la Junta de Personal, una vez formadas la Mesas Electorales, que se constituyen como órganos soberanos supervisores de todo el proceso electoral, éstas obtendrán de la Administración el censo de funcionarios y confeccionarán con los medios que les habrá de facilitar la Administración Pública correspondiente, la lista de electores. Serán las Mesas electorales las que harán público entre los trabajadores el censo, con identificación de los electores, y las que resolverán las reclamaciones que se presenten relativas a inclusiones, exclusiones o correcciones.
A la vista de la regulación anteriormente señalada se desprende que el envío del censo de funcionarios se debe facilitar, única y exclusivamente, a las Mesas Electorales.
En consecuencia, la cesión de datos personales de los funcionarios docentes a las Centrales Sindicales no estaría exenta de la necesidad de solicitar el consentimiento, ya que la Ley no contempla posibilidad de que el censo de funcionarios electores se facilite directamente por la Unidad de Personal correspondiente, en este caso la Dirección General de Recursos Humanos de la Consejería de Educación, a las Centrales Sindicales promotoras del procedimiento electoral.

¿Puede publicarse en el tablón del Departamento correspondiente de un Instituto de Enseñanza Secundaria la hoja del horario individual de un profesor incluyendo los datos personales de dirección personal, DNI, número de teléfono, fecha de nacimiento, antigüedad en el cuerpo y número de registro personal? ¿Y sus faltas de asistencia?

La publicación en el tablón del Departamento correspondiente de un Instituto de Enseñanza Secundaria de la hoja del horario individual de un profesor, incluyendo los datos personales de dirección personal, DNI, número de teléfono, fecha de nacimiento, antigüedad en el cuerpo y número de registro personal, incluiría datos excesivos, que nada interesan a la finalidad de informar sobre el horario del profesor y así poder realizar el control diario sobre el cumplimiento de su horario y comprobar la correcta aplicación de los criterios pedagógicos que establece el Claustro, evitándose presuntos favoritismos o discriminaciones.
Sólo se deben publicar para la finalidad mencionada los datos del nombre y apellido del profesor y sus datos referidos a los criterios de elección de horario que establece la normativa aplicable, esto es: su categoría académica, la antigüedad en el cuerpo, la antigüedad en el Instituto, el último criterio de desempate fijado en la convocatoria del concurso de traslados, y los criterios pedagógicos establecidos en el Claustro.
Por otra parte, la exposición de la copia de los partes de faltas de asistencia de los docentes en la sala de profesores o en otros lugares de acceso público de acuerdo con el procedimiento establecido en las correspondientes "Instrucciones" sobre organización y funcionamiento dictadas por la Consejería de Educación, incluyendo sus datos personales y el motivo literal de la falta de asistencia, no resulta conforme

con la normativa sobre protección de datos. A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, dichos datos de carácter personal deberían ser conocidos únicamente por la Dirección del Centro, por la Dirección del Área Territorial y por la Inspección.
En estos términos, la publicación de los referidos partes de asistencia, en la medida en que puedan ser conocidos por terceros, podría constituir una vulneración de los principios de protección de datos de acuerdo a lo dispuesto en el artículo 10 de la LOPD, que regula el deber de secreto estableciendo 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".
Ello es así porque la publicación prevista en las "Instrucciones" sobre organización y funcionamiento, dictadas a estos efectos por la Administración educativa, no deriva de ninguna habilitación legal.
Por consiguiente, dar publicidad en un lugar visible a los datos de carácter personal que estén reflejados en los partes de asistencia de los profesores puede suponer una vulneración del deber de secreto del artículo 10 de la LOPD, debiendo en consecuencia procederse a la modificación de las "Instrucciones" a la que nos venimos refiriendo, de manera que dicha publicación no pueda realizarse en el futuro.
No obstante lo anterior, hay que tener en cuenta que los/as Directores/as de los centros de enseñanza públicos deben cumplir con la normativa vigente, contenida en las Instrucciones a la que nos venimos refiriendo, existiendo una relación jerárquica entre la Administración educativa y el centro docente que es necesario preservar, puesto que según dispone el artículo 21.1 Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los órganos administrativos podrán dirigir las actividades de sus órganos jerárquicamente dependientes mediante instrucciones y órdenes de servicio, y el incumplimiento de las mismas puede derivar en responsabilidad disciplinaria del titular del órgano subordinado.
En consecuencia, desde la Agencia de Protección de Datos de la Comunidad de Madrid se ha instado a la Administración educativa para que proceda a modificar sus "Instrucciones" sobre organización y funcionamiento, de manera que en futuras Instrucciones no se contemple la obligación de publicar los partes faltas de asistencia de los profesores.

¿Puede un Instituto de Educación Secundaria publicar en la página Web del Centro el nombre de los profesores que imparten enseñanzas y el horario de atención a las consultas de los padres?

Según prevé el artículo 6 de la LOPD, el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado. Sin embargo, no será preciso dicho consentimiento para recoger datos de carácter personal si así viene establecido en una ley o cuando se recojan en el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
Asimismo, la LOPD establece en el artículo 11.1 que "Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Así pues, la norma general para que exista la posibilidad de cesión de datos es que los afectados, por ellos mismos, consientan en que esa cesión pueda efectuarse y que la misma persiga un fin legítimo entre cedente y cesionario. Sin embargo, dicha norma general del consentimiento no es absoluta y así, el propio artículo 11 regula -en su apartado 2-

una serie de excepciones a la misma, entre las que se encuentra la referente a que una Ley ampare expresamente la cesión.
La publicación de los datos de nombre del profesor y el horario de atención constituye una cesión de datos, ya que el artículo 3 i) de la LOPD define la cesión como "toda revelación de datos realizada a una persona distinta del interesado". Además, dicha cesión se realiza de forma indiscriminada, dado que cualquier persona que acceda a la página puede recabar esta información sin necesidad de tener ningún tipo de interés legítimo en su conocimiento. Por tanto, dicha cesión requiere que la comunicación se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y el cesionario y que el interesado preste su consentimiento, según prevé el artículo 11.1 de la LOPD, salvo que se den alguna de las excepciones previstas en el apartado 2, excepciones que en el presente caso no se presentan.
Por otra parte, debe estarse a lo previsto en la Instrucción de la Viceconsejería de Educación, sobre la inclusión en el portal Educamadrid de las páginas o sitios Web de los centros y servicios educativos, en cuyo apartado 8 se indica expresamente que "(…) el Director del centro debe contar con el consentimiento por escrito, según el formato que se incluye en el Anexo II, de todas las personas cuya imagen y otros datos personales (nombre, correo electrónico…) aparezcan en las páginas Web, siempre que a través de ellos se les pueda identificar (…)".
En consecuencia, podemos afirmar que, cumpliendo con la exigencia del consentimiento previsto en la LOPD, en la Instrucción de la Viceconsejería de Educación sobre la inclusión en el Portal Educamadrid de las páginas o sitios Web de los centros y servicios educativos, se establece la obligación de obtención del consentimiento previo de cualquier afectado cuyos datos personales quieran incluirse en la página Web del centro, y se prevé un modelo para la prestación de dicho consentimiento, no siendo posible la publicación de los datos personales en caso contrario.
Asimismo, y respecto de la inclusión del horario de atención del profesorado a las consultas de los padres de alumnos, se podrá incluir dicha información si no va asociada a ningún dato de carácter personal de un profesor. Si ello no fuera posible, se deberá contar con el consentimiento previo de este.

¿Se puede publicar en Internet el directorio: nombres y datos profesionales de contacto de todo el personal de un Centro Educativo?

En el artículo 23 (Publicación de Directorios) de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Web institucionales y en otros medios electrónicos y telemáticos, se aborda con amplitud esta cuestión.
Sin lugar a dudas, la publicación de directorios de los empleados públicos, con datos identificativos relativos, entre otros, al puesto de trabajo desempeñado, la dirección postal del mismo, la dirección de correo electrónico o el número de teléfono profesional, constituye una forma de tratamiento de datos de carácter personal.
El artículo 35 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece únicamente el derecho de los ciudadanos a identificar a las autoridades y al personal de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos, pero no habilita la publicación de Listados de Puestos de Trabajo de los empleados públicos.
De conformidad con el artículo 74 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, las Administraciones Públicas estructuran su organización a través de relaciones de puestos de trabajo u otros instrumentos organizativos similares

que comprenden, al menos, la denominación de los puestos, los grupos de clasificación profesional, los cuerpos o escalas, en su caso, a que estén adscritos los sistemas de provisión y las retribuciones complementarias. Las relaciones de puestos de trabajo así como los instrumentos organizativos similares son públicos.
Salvo habilitación legal expresa que así lo autorice, la publicación de las relaciones de puestos de trabajo en los Boletines o Diarios Oficiales en Internet no deberá contener los datos del nombre y apellidos, ni ningún otro dato de carácter personal de los empleados públicos que ocupen cada uno de los puestos de trabajo comprendidos en dichas relaciones de puestos de trabajo u otros instrumentos organizativos.
Atendiendo a que la aplicación del artículo 35 b) de la Ley 30/1992, de 26 de noviembre, tiene lugar cuando el ciudadano ostenta la condición de interesado en un procedimiento administrativo, y en evitación del tratamiento masivo de los datos personales de los afectados, con carácter general se recomienda que no se publiquen en los sitios Web institucionales, o en otros canales electrónicos o telemáticos, la dirección de correo electrónico ni el número de teléfono de los empleados públicos al servicio de la Administración pública, recomendándose la publicación de números de teléfono y direcciones de correo electrónico institucionales.
De acuerdo con la Recomendación 2/2008, de 25 de abril, de la APDCM, en la publicación de las Relaciones de Puestos de Trabajo se recomienda que no se proceda a divulgación de datos personales, dado que dicha publicación sería excesiva, no adecuada y contraria al principio de calidad de datos, establecido en los artículos 4 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre.
En consecuencia, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda que, en su caso, la publicación de los datos personales que componen los Directorios institucionales, se realice a través de una Intranet administrativa, o de un área privada ubicada en el sitio Web institucional o en el canal electrónico o telemático abierto en Internet, que requieran la identificación y autenticación por mecanismos fiables que permitan acreditar indubitadamente la identidad de la persona que acceda a dicha información.
No obstante lo anterior, en el supuesto del personal con responsabilidades políticas, la Agencia de Protección de Datos de la Comunidad de Madrid entiende que puede procederse a la publicación de su nombre y apellidos, dirección postal, y dirección de correo electrónico, sin consentimiento del mismo, atendiendo al principio democrático y representativo. La dirección de correo electrónico personal podrá ser sustituida en estos casos por una dirección de correo electrónico institucional.
Con carácter excepcional, cuando concurra el interés público necesario, corresponderá al titular del órgano administrativo determinar, en su caso, la conveniencia de proceder a la publicación sin restricciones en el sitio Web institucional o en el canal electrónico o telemático abierto en Internet, de los datos referentes al nombre y apellidos, denominación del puesto, teléfono y/o dirección de correo electrónico de sus empleados públicos con responsabilidad meramente administrativa.

¿Se pueden obtener datos de los profesores del fichero de gestión de personal docente a los efectos de enviar información sobre las convocatorias de cursos para la formación del profesorado dependiente de la Consejería de Educación?

De acuerdo con la normativa aplicable en materia de ecuación, las Administraciones educativas deben promover la actualización y la mejora continua de la cualificación profesional de los profesores y la adecuación de sus conocimientos y métodos a la evolución de la ciencia. Asimismo, las Administraciones deben fomentar la formación permanente del profesorado, teniendo los profesores el deber de realizar periódicamente actividades de actualización científica, didáctica y profesional en los centros docentes, en instituciones formativas específicas, en las universidades y, en el

caso del profesorado de formación profesional, también en las empresas. Las Administraciones educativas deben planificar las actividades necesarias de formación permanente del profesorado y garantizar una oferta diversificada y gratuita de estas actividades, estableciéndose las medidas oportunas para favorecer la participación del profesorado en estos programas.
En el ámbito de la Comunidad de Madrid, la competencia para la planificación y desarrollo de los programas y actividades de formación permanente del profesorado le corresponde a la Consejería de Educación. Dicha Consejería, en cuanto Administración Pública Educativa, debe velar y cumplir con el principio de formación del profesorado, competencia que le faculta para poder informar a todos los profesores de su ámbito territorial de las convocatorias de formación para cada curso, teniendo en cuenta que no sólo es una responsabilidad de la Administración Pública, sino de todos los profesores, que tienen -a su vez- la obligación legal de formarse.
De esta manera, al tratarse del ejercicio de una competencia administrativa propia, la Dirección General competente no precisaría el consentimiento de los profesores para utilizar los datos del fichero de gestión de personal docente.
Sin embargo, debe precisarse que los datos que se obtendrán del fichero serán los necesarios para enviar la información correspondiente a convocatorias de formación para el curso, atendiendo así al principio de calidad de los datos.

¿Puede un centro docente de la Comunidad de Madrid ceder datos de los profesionales no funcionarios a un Colegio Oficial de la Comunidad de Madrid?

Sí. Y ello con base en que los Colegios Profesionales tienen como fin esencial, entre otros, ordenar el ejercicio de las profesiones, siendo la colegiación un requisito indispensable para el ejercicio de la profesión. Además, una de las finalidades de los Colegios Profesionales es ordenar con normas propias la actividad de los colegiados. Así, en los Estatutos del Colegio se establece la obligatoriedad de estar colegiado, salvo el profesorado sometido a la función pública.
Por tanto, para que el Colegio Profesional pueda cumplir con estas obligaciones establecidas en la Ley 19/1997 y en sus respectivos estatutos, los centros docentes pueden comunicarle los datos de los profesionales no funcionarios sin contar con el consentimiento de los afectados, ya que concurriría la excepción al consentimiento prevista en el artículo 11.2.c) de la LOPD, esto es, que el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implica necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
En este sentido, el artículo 5 de dicha Ley establece las competencias del Colegio. Entre ellas, cabe destacar las siguientes:
a) Ordenar con normas propias la actividad de los colegiados.
b) Ejercer la representación y defensa de la profesión en el ámbito de la Comunidad de Madrid, incluyendo sus funciones profesionales ante la Administración, Instituciones, Tribunales, entidades y particulares con legitimación para ser parte en todos los litigios que afecten a los intereses profesionales y con la posibilidad de ejercer el derecho de petición de conformidad con la Ley y de impulsar todas reformas legislativas que considere justas en defensa de la profesión.
c) Adoptar las medidas necesarias para evitar el intrusismo profesional y la competencia desleal dentro del ámbito de la profesión llevando a cabo las actuaciones que sean necesarias.
d) Colaborar con los directores de Centros de Enseñanza Privada para asegurar el cumplimiento de los requisitos del ejercicio profesional: Titulación y Colegiación. Para

ello solicitarán durante el primer trimestre de cada curso el cuadro de profesores del Centro con el número respectivo de colegiación, la materia que imparten y el horario. No obstante, solo se deben facilitar al Colegio Profesional aquellos datos necesarios para cumplir las obligaciones previstas en la Ley 19/1997, de 11 de julio, de Colegios Profesionales en la Comunidad de Madrid, y en sus respectivos estatutos. Así, por ejemplo, cuando la finalidad de la cesión sea conocer la obligación o no de la colegiación. En sentido contrario, el dato del horario del profesor no habría que facilitarlo porque sería excesivo respecto de la finalidad que se pretende.

Cesiones de datos derivadas de otras actuaciones en el ámbito educativo

¿Pueden publicarse en la página Web de la Consejería de Educación los listados de los participantes en procesos selectivos que tengan lugar?

La publicación de listados de personas que estén participando en un proceso selectivo ante cualquier Administración Pública es obligatoria en cumplimiento del principio de publicidad que rige todas las convocatorias de pruebas selectivas. En este sentido el artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, viene a establecer que la práctica de la notificación, cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo, se realizara mediante la publicación del acto. A su vez, cabe citar el artículo 1.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, cuando dispone que las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en dicha Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.
En el artículo 4 de la propia Ley 11/2007, de 22 de junio, se prevé que la utilización de las tecnologías de la información tendrá las limitaciones establecidas por la Constitución y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos, y ajustándose, entre otros principios, al respeto al derecho a la protección de datos de carácter personal en los términos establecidos por la LOPD, en las demás leyes específicas que regulan el tratamiento de la información y en sus normas de desarrollo, así como a los derechos al honor y a la intimidad personal y familiar.
El artículo 14 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Webs institucionales y en otros medios electrónicos y telemáticos, establece que "Entre otros procedimientos, se reputan procedimientos de concurrencia competitiva los procesos selectivos para el ingreso de empleados públicos en la Administración pública y los de provisión de puestos de trabajo de empleados públicos, los relativos a la obtención de premiso extraordinarios y becas, los relativos a contratos administrativos, y los relativos a la obtención de plazas en colegios públicos o concertados y en las Universidades públicas, así como aquellos otros en los que existiendo una pluralidad de solicitantes y un número de plazas o de créditos limitados, deba procederse a la asignación de los mismos en función de la consideración de unos méritos o requisitos susceptibles de cómputo o valoración".
Así mismo, se reitera que la publicación de datos personales en Boletines o Diarios Oficiales en Internet derivada de los procedimientos de concurrencia competitiva se fundamenta en el artículo 59.6. b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
En todos estos casos, el órgano administrativo titular de la competencia administrativa del procedimiento de concurrencia competitiva correspondiente, deberá decidir sobre los datos personales que sean objeto de publicación con acceso no identificado por cualquier persona, debiendo producir dicha publicación la menor injerencia posible sobre el derecho a la intimidad y a la protección de los datos de carácter personal de los ciudadanos afectados.
En este tipo de supuestos, se recomienda que el acceso no identificado por cualquier persona, realizado como consecuencia de la publicación de datos personales en Boletines y Diarios Oficiales en Internet, se limite a los datos personales mínimos correspondientes al resultado final del procedimiento administrativo, a la indicación de

los datos personales mínimos de los beneficiarios o adjudicatarios de dicho procedimiento, así como -en su caso- a la publicación de la baremación total de los méritos valorados.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, se cumple así suficientemente con las exigencias derivadas de lo dispuesto en el artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, causando esta publicación una menor injerencia en la intimidad de los ciudadanos afectados por el tratamiento de sus datos.
La Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación de actos administrativos de trámite referentes a procedimientos de concurrencia competitiva en Boletines o Diarios Oficiales en Internet o en sitios Web institucionales sea sustituida por la utilización de un espacio privado, con acceso restringido, en los sitios Web institucionales.
Así, por ejemplo -entre otros datos de carácter personal contenidos en los actos administrativos de trámite-, cuando los procedimientos de concurrencia competitiva incorporen algún trámite administrativo consistente en la realización de una baremación parcial de los méritos de los ciudadanos afectados, se recomienda que se proceda a la publicación de los resultados de la baremación parcial a través de este espacio privado, con acceso restringido, en los sitios Web institucionales, en el canal electrónico o telemático abierto en Internet, en los tablones de anuncios electrónicos, o, en su caso, en la correspondiente Intranet administrativa.
La utilización de estos espacios privados garantizará que los participantes en dichos procedimientos puedan conocer los actos administrativos derivados de la tramitación del expediente identificándose mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios como el uso de un nombre de usuario y una contraseña segura, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
Siguiendo lo establecido en la citada Recomendación 2/2008, de 25 de abril, de la APDCM, para la publicación en los sitios Web institucionales, sin restricción ni identificación de acceso, de actos administrativos de trámite derivados de procedimientos de concurrencia competitiva que contengan datos de carácter personal de los ciudadanos afectados, se recomienda que el Órgano competente obtenga el consentimiento previo y expreso de los mismos.
De acuerdo con lo indicado anteriormente, en caso de no obtenerse este consentimiento, se recomienda que la publicación de dichos actos administrativos de trámite se realice únicamente en espacios privados de los tablones de anuncios electrónicos, del sitio Web institucional, o del canal electrónico o telemático abierto en Internet, o, en su caso, en la correspondiente Intranet administrativa, exigiéndose la acreditación indubitada de la identidad de la persona que acceda a los datos mediante el uso de cualquiera de los medios de identificación señalados en los apartados anteriores.
Especialmente, cuando los procedimientos de concurrencia competitiva incorporen algún dato de carácter personal relativo a la existencia de discapacidades físicas, psíquicas o sensoriales de los afectados, se recomienda que se proceda únicamente a la publicación de los resultados mínimos correspondientes a la baremación efectuada.
En estos supuestos, se recomienda que, de acuerdo con lo dispuesto en el artículo 61 de la Ley 30/1992, de 26 de noviembre, por parte de la Administración pública u Órgano administrativo competente, se proceda -en la medida de lo posible- a la publicación de una somera indicación del contenido de dicha baremación y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para el conocimiento íntegro de la misma y constancia de tal conocimiento.

A su vez, en el caso de que se publiquen en los sitios Web institucionales datos relativos a actos administrativos de procedimientos de concurrencia competitiva que a su vez hayan sido publicados en el Boletín o Diario Oficial correspondiente a través de Internet, la publicación en los referidos sitios deberá limitarse a establecer una referencia o enlace a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original - por ejemplo, vía RSS -, u otros mecanismos similares, sin necesidad de duplicar la información.
Finalmente, se recomienda que, una vez finalizado el plazo para interponer las reclamaciones y/o recursos administrativos legalmente establecidos, se proceda a la supresión y borrado físico de la información de carácter personal publicada en el sitio Web institucional, en los tablones de anuncios electrónicos, en el canal electrónico o telemático abierto en Internet, o en la correspondiente Intranet administrativa, referente al procedimiento de concurrencia competitiva.
De manera específica, en relación con la publicación de datos personales derivados de procesos selectivos de acceso a la función pública, en el artículo 15 de la Recomendación 2/2008, de la APDCM, se establece:
"15.1 La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, determina en su artículo 61 los sistemas selectivos de acceso a la función pública. En el caso de los funcionarios de carrera serán los de oposición y concurso-oposición, teniendo el sistema de concurso un carácter excepcional. En el supuesto del personal laboral fijo, los sistemas selectivos serán la oposición, el concurso-oposición y el concurso de valoración de méritos. De conformidad con el artículo 55 de la citada Ley, estos procedimientos de concurrencia competitiva se ajustan, entre otros, a los principios de publicidad de las convocatorias y de sus bases.
15.2 Los artículos 15 a 26, del Real Decreto 364/1995, de 10 de marzo, por el que se aprueba el Reglamento General de Ingreso del Personal al Servicio de la Administración General del Estado y de Provisión de Puestos de Trabajo y Promoción Profesional de los Funcionarios Civiles del Estado, aplicable a los procesos selectivos de la Administración de la Comunidad de Madrid, regulan los trámites administrativos de los procesos selectivos de acceso a la función pública, contemplando aquellos trámites y actos administrativos que serán objeto de publicación en el Boletín o Diario Oficial correspondiente.
Entre los trámites administrativos objeto de publicación con datos de carácter personal se encuentran los referentes a las listas de admitidos y excluidos, la relación de aprobados y el nombramiento como funcionarios de carrera.
15.3 La Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación en relación con estos procedimientos en los Boletines o Diarios Oficiales en Internet, se produzca únicamente en relación con los datos relativos al nombre, apellidos, número del Documento Nacional de Identidad, puntuación total obtenida y nombramiento como funcionarios de carrera de las personas que obtuvieron las plazas. Asimismo, se recomienda la aplicación de esta norma cuando se trate de procesos de acceso a la Administración pública que afecten a personal laboral.
Especialmente, se recomienda que, en ningún caso, se proceda a la publicación en el Boletín o Diario Oficial en Internet de los datos de carácter personal de aquellos aspirantes que no hayan superado dicho proceso.
En el supuesto de que, apartándose del contenido de estas recomendaciones, se produjese la publicación de los listados de excluidos provisionales o definitivos en los Boletines o Diarios Oficiales en Internet, así como las causas de exclusión, dicha publicación deberá realizarse de manera que cause la menor injerencia sobre el derecho a la intimidad y a la protección de datos de los ciudadanos afectados.
A su vez, en relación con la publicación de la relación definitiva de aprobados, debe tenerse en cuenta que la minusvalía es un dato de salud, por lo que se recomienda

que la publicación de dicha relación contenga la información mínima relativa al hecho de la discapacidad, sin incluir referencia alguna al grado o el tipo de la misma.
15.4 La Agencia de Protección de Datos de la Comunidad de Madrid, recomienda que los actos de trámite que contengan datos de carácter personal en los procesos selectivos, y, en especial, los referentes a las calificaciones obtenidas por los aspirantes en los distintos exámenes y pruebas realizadas, las adaptaciones concedidas a dichos aspirantes que concurran por el turno de discapacidad y la convocatoria de los aspirantes para realizar los exámenes o proceder a la lectura de los mismos, se publiquen únicamente a través de un sitio Web institucional, en un canal electrónico o telemático de la Administración u Órgano administrativo convocante, o bien en el tablón de anuncios electrónico del Órgano competente, con acceso identificado y restringido a los interesados, exigiéndose la acreditación indubitada de la identidad mediante el uso de cualquiera de los medios de identificación señalados en esta Recomendación, acreditándose indubitadamente la identidad de la persona que realice el acceso a través de los mismos.
A través de dichos sistemas de acceso deberá garantizarse que únicamente los interesados en el procedimiento selectivo podrán acceder a los datos personales de terceras personas relacionados con dicho procedimiento, exigiéndose, como requisito indispensable, de la identificación y autenticación del ciudadano que realice dicho acceso, mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios, como la introducción de una clave de acceso personalizada previamente asignada por la Administración, con su correspondiente contraseña, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
15.5 Sin perjuicio de lo dispuesto en los apartados anteriores, se podrá proceder a la publicación de los citados trámites en el sitio Web de la Administración u Órgano administrativo convocante, sin la exigencia de un sistema de acceso identificado o restringido, en aquellos supuestos en que se solicite con carácter previo el consentimiento para dicha publicación a los aspirantes. A dichos efectos se considera que este consentimiento debe ser diferente del consentimiento que presta el aspirante para participar en el proceso selectivo. Para la solicitud de dicho consentimiento se estima como medio idóneo para la obtención del mismo su solicitud y obtención a través del modelo utilizado por el ciudadano afectado para participar en el proceso selectivo correspondiente.
En estos supuestos, se recomienda que en la Orden o Resolución que convoque el procedimiento de acceso a la función pública o de ingreso como empleado público, se contemple dicha forma de publicación de los distintos actos de trámite.
15.6 En relación con los aspirantes que se presenten a un proceso selectivo por el turno de discapacidad, será suficiente para cumplir con los principios de publicidad y concurrencia que los mismos sean identificados, ya sea en las listas de admitidos y excluidos, en la relación de aprobados o en su nombramiento, con la letra "D", sin necesidad de publicar el tipo de discapacidad, ni el grado de la misma.
En consecuencia, se recomienda que se evite la referencia expresa al tipo de discapacidad o al grado de la misma, por resultar contraria a lo dispuesto en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, ya que los datos sobre minusvalía tienen la consideración de datos especialmente protegidos.
15.7 En el supuesto de que se pretendan publicar en un sitio Web institucional los actos administrativos que hayan aparecido en los Boletines o Diarios Oficiales en Internet en relación con un proceso selectivo, la Administración u Órgano administrativo competente deberá limitarse a establecer una referencia o enlace a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original -por ejemplo, vía RSS-, u otros mecanismos similares, sin necesidad de duplicar la información.

15.8 De conformidad con el principio de finalidad, una vez concluido el procedimiento administrativo que justificó su publicación y transcurrido el plazo previsto para la interposición, en su caso, de las correspondientes acciones y/o reclamaciones legales, deberá procederse a la cancelación de los datos de carácter personal de trámite, tales como los relativos a los excluidos a las pruebas selectivas, a la mención de la causa de exclusión, y a las calificaciones parciales correspondientes a las diferentes pruebas realizadas del sitio Web institucional, canal electrónico o telemático administrativo, o tablón de anuncios electrónico de la Administración u Órgano administrativo convocante.
En concreto, se recomienda que por parte de la Administración pública u Órgano administrativo competente no se proceda a la conservación y mantenimiento de la publicación de datos personales relativos al tratamiento histórico de los actos de trámite de las convocatorias de procesos selectivos, por reputarse dicha forma de tratamiento contraria a la normativa sobre protección de datos".
En otro orden de cosas, conviene señalar que los listados generados a consecuencia de la publicación de los datos personales a los que se refiere la pregunta, no constituyen fuentes de acceso público, aunque su inclusión en los Boletines Oficiales correspondientes, que sí son una fuente de acceso público, permite que sean consultados y tratados por terceras personas. En estos casos, el propio artículo 6 LOPD establece que los datos que figuren en una fuente de acceso público podrán tratarse sin el consentimiento de los afectados, pero siempre que su tratamiento sea necesario para satisfacer un interés legitimo del responsable del fichero, teniendo en cuenta que éste tendrá que cumplir con la obligación del deber de información al afectado establecido en el artículo 5.4 de la LOPD.
A los efectos de evitar que los listados sean copiados y alojados en servidores ajenos, se plantea la posibilidad de incluir la siguiente leyenda informativa:
"Los listados que se publican en esta página Web y que contienen datos de carácter personal se ajustan a la legislación de protección de datos y su única finalidad, de conformidad con lo previsto en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, es la de proceder a notificar a cada uno de los aspirantes el contenido del procedimiento selectivo. Estos listados no constituyen fuente de acceso público y no podrán ser reproducidos ni en todo ni en parte, ni transmitidos ni registrados por ningún sistema de recuperación de información, sin el consentimiento de los propios afectados."
Igualmente se señala que, en este caso y en todos aquellos en que se soliciten datos personales, se deberá dar cumplimiento explícito al derecho de información previo al tratamiento de los datos, de conformidad con lo previsto en el artículo 5 de la LOPD, debiéndose informar de la existencia del fichero, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección del responsable del fichero. En este sentido, y al objeto de cumplir con el deber de información, conforme al artículo 5.1 de la LOPD, en aquellos modelos o solicitudes a través de los cuales se recaben datos de carácter personal deberá aparecer un texto informativo que cumpla plenamente con lo previsto en dicho precepto legal.

¿Cómo debe procederse en la publicación de los datos personales de los alumnos beneficiarios y excluidos en la Convocatoria de ayudas de libros de texto y material didáctico?

Por la Secretaría General Técnica de la Consejería de Educación de la Comunidad de Madrid se remitió, para su preceptivo informe, el Proyecto de Orden de bases reguladoras y convocatoria de dichas ayudas para el curso escolar 2008/2009.
Analizado el Proyecto de Orden se informó lo siguiente:

(…)
El Proyecto de Orden tiene por objeto el establecimiento de las bases que regularán la concesión, por la Consejería de Educación, de becas de libros de texto y material didáctico par el curso escolar 2008/2009 (Capítulo I), así como la convocatoria de dichas ayudas (Capítulo II). A través de esta Orden se pretenden conceder, en régimen de concurrencia competitiva, las correspondientes ayudas, que deberán ser solicitadas por los padres o tutores legales de los alumnos que en el año escolar 2008/2009 vayan a cursar estudios de las etapas educativas que se señalan en la propia Orden, utilizando para ello el modelo que se acompaña como ANEXO ÚNICO.
De acuerdo con lo dispuesto en su artículo 3.2, a los efectos previstos en la Orden, se considerará familia numerosa aquella que se encuentre en posesión del título administrativo en vigor que la acredite como tal, por estar integrada por el número de miembros que determina la Ley 40/2003, de 18 de noviembre, de Protección a las Familias Númerosas.
Con carácter general la concesión de las ayudas se realizará en función de la "Determinación de la renta per cápita familiar (artículo 4)". Ello no obstante, no será necesario acreditar la renta cuando se trate de beneficiarios de ayudas de libros concedidas por la Consejería de Educación para el curso 2007/2008 en la modalidad de "Beneficiarios del MEC".
Según disponen los artículos 4.6 y 7.3 (apartados b y c), en el supuesto en que ninguno de los miembros de la unidad familiar genere ingresos con deducción de IRPF, la situación económica deberá acreditarse mediante informe de vida laboral positivo, acompañado del correspondiente certificado del empleador. Por su parte, los supuestos de carencia económica se justificarán mediante documento expedido por los servicios sociales municipales, debidamente firmado y sellado, en el que conste la intervención de dichos servicios sociales y, si fuera posible, la cantidad estimada de ingresos anuales de que dispone la unidad familiar, o bien, mediante indicación expresa en el modelo de solicitud de que la unidad familiar es beneficiaria de la renta mínima de inserción (RMI) para su comprobación de oficio por la Comunidad de Madrid.
Las solicitudes deberán cumplimentarse en el modelo correspondiente (artículo 6.1), que se acompaña como ANEXO ÚNICO de la Orden. La presentación de la solicitud implica la autorización para que la Consejería de Educación pueda obtener, a través de la Agencia Estatal de la Administración Tributaria, la información necesaria para determinar la renta de la unidad familiar.
Del mismo modo, la presentación de la solicitud supone la declaración, por parte del solicitante de no hallarse incurso en ninguno de los supuestos recogidos en el artículo 13.2 de la Ley General de Subvenciones.
Las solicitudes deberán acompañarse de la documentación referida en el artículo 8 del Proyecto de Orden, que establece tres tipos de modalidades, a saber:
a) Familias cuyos hijos hayan percibido en 2007 ayudas de libros en la modalidad de beneficiario del MEC.
b) Familias númerosas.
c) Resto de familias (modalidad general).
De acuerdo con los tipos anteriores, se exigirá la presentación de diversa documentación, entre la que destaca la presentación del "Título de familia númerosa", DNI o NIE, "Libro de familia completo", número de teléfono móvil y dirección de correo electrónico. A su vez, en los supuestos específicos a los que se hace mención en la Orden será necesaria la presentación del pasaporte, permiso de residencia y/o certificado de empadronamiento, así como, en su caso, la presentación de la documentación acreditativa de la incapacitación judicial (sentencia judicial), de la discapacidad (resolución administrativa de reconocimiento de grado de minusvalía), y/o la acreditación de la situación económica en los supuestos de carencia de ingresos

con deducción del IRPF mediante la documentación a la que se ha hecho mención anteriormente.
De otra parte, de acuerdo con lo dispuesto en los artículos 10 y 12 de la Orden se procederá, respectivamente, a la elaboración de las listas provisionales de admitidos y excluidos, que se expondrá en los tablones de anuncios de las Direcciones de Área Territorial, en la Oficina de Información de la Consejería de Educación y en los respectivos Centros, con indicación de los alumnos excluidos provisionalmente y de las causas de su exclusión, y al dictado de la resolución definitiva, con indicación de la lista definitiva de beneficiarios y excluidos, que se hará pública en los tablones de anuncios de las Direcciones de Área Territorial, en los centros docentes, en la Oficina de Información de la Consejería de Educación y en la página Web www.madrid.org. Asimismo, la resolución de la convocatoria se publicará en el BOCM.
En concreto, la resolución de la convocatoria expresará el nombre y apellidos de los alumnos beneficiarios, el municipio y centro docente de referencia y el importe de la ayuda, diferenciando si lo son por su pertenencia a familia númerosa, por haber percibido la ayuda en el curso 2007/2008 en la modalidad de beneficiarios del Ministerio de Educación y Ciencia o por el nivel de renta. La resolución detallará, asimismo, las solicitudes de ayuda denegadas, en cuya relación figurará la causa que haya motivado la no obtención de la misma.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, de acuerdo con la normativa administrativa aplicable, este tipo de procedimientos han de reputarse como procedimientos de concurrencia competitiva, toda vez que existiendo una pluralidad de solicitantes y un número de plazas o de créditos limitados, debe procederse a la asignación de los mismos en función de la consideración de unos méritos o requisitos susceptibles de cómputo o valoración.
Siguiendo lo previsto en el artículo 14.2 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Webs institucionales y en otros medios electrónicos y telemáticos, "La publicación de datos personales en Boletines o Diarios Oficiales en Internet derivada de los procedimientos de concurrencia competitiva se fundamenta en el artículo 59.6. b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".
En estos casos, el órgano administrativo titular de la competencia administrativa del procedimiento de concurrencia competitiva correspondiente, deberá decidir sobre los datos personales que sean objeto de publicación con acceso no identificado por cualquier persona, debiendo producir dicha publicación la menor injerencia posible sobre el derecho a la intimidad y a la protección de los datos de carácter personal de los ciudadanos afectados.
En este tipo de supuestos, se recomienda que el acceso no identificado por cualquier persona, realizado como consecuencia de la publicación de datos personales en Boletines y Diarios Oficiales en Internet, se limite a los datos personales mínimos correspondientes al resultado final del procedimiento administrativo, a la indicación de los datos personales mínimos de los beneficiarios o adjudicatarios de dicho procedimiento, así como -en su caso- a la publicación de la baremación total de los méritos valorados.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, se cumple así suficientemente con las exigencias derivadas de lo dispuesto en el artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, causando esta publicación una menor injerencia en la intimidad de los ciudadanos afectados por el tratamiento de sus datos.

A su vez, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación de actos administrativos de trámite referentes a procedimientos de concurrencia competitiva en Boletines o Diarios Oficiales en Internet o en sitios Web institucionales sea sustituida por la utilización de un espacio privado, con acceso restringido, en los sitios Web institucionales.
Así, por ejemplo -entre otros datos de carácter personal contenidos en los actos administrativos de trámite-, cuando los procedimientos de concurrencia competitiva incorporen algún trámite administrativo consistente en la realización de una baremación parcial de los méritos de los ciudadanos afectados, se recomienda que se proceda a la publicación de los resultados de la baremación parcial a través de este espacio privado, con acceso restringido, en los sitios Web institucionales, en el canal electrónico o telemático abierto en Internet, en los tablones de anuncios electrónicos, o, en su caso, en la correspondiente Intranet administrativa.
La utilización de estos espacios privados garantizará que los participantes en dichos procedimientos puedan conocer los actos administrativos derivados de la tramitación del expediente identificándose mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios como el uso de un nombre de usuario y una contraseña segura, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
Para la publicación en los sitios Web institucionales, sin restricción ni identificación de acceso, de actos administrativos de trámite derivados de procedimientos de concurrencia competitiva que contengan datos de carácter personal de los ciudadanos afectados, se recomienda que el Órgano competente obtenga el consentimiento previo y expreso de los mismos.
De acuerdo con lo indicado anteriormente, en caso de no obtenerse este consentimiento, se recomienda que la publicación de dichos actos administrativos de trámite se realice únicamente en espacios privados de los tablones de anuncios electrónicos, del sitio Web institucional, o del canal electrónico o telemático abierto en Internet, o, en su caso, en la correspondiente Intranet administrativa, exigiéndose la acreditación indubitada de la identidad de la persona que acceda a los datos mediante el uso de cualquiera de los medios de identificación señalados en los apartados anteriores.
Especialmente, cuando los procedimientos de concurrencia competitiva incorporen algún dato de carácter personal relativo a la existencia de discapacidades físicas, psíquicas o sensoriales de los afectados, se recomienda que se proceda únicamente a la publicación de los resultados mínimos correspondientes a la baremación efectuada.
En estos supuestos, se recomienda que, de acuerdo con lo dispuesto en el artículo 61 de la Ley 30/1992, de 26 de noviembre, por parte de la Administración pública u Órgano administrativo competente, se proceda -en la medida de lo posible- a la publicación de una somera indicación del contenido de dicha baremación y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para el conocimiento íntegro de la misma y constancia de tal conocimiento.
En el caso de que se publiquen en los sitios Web institucionales datos relativos a actos administrativos de procedimientos de concurrencia competitiva que a su vez hayan sido publicados en el Boletín o Diario Oficial correspondiente a través de Internet, la publicación en los referidos sitios deberá limitarse a establecer una referencia o enlace a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original - por ejemplo, vía RSS -, u otros mecanismos similares, sin necesidad de duplicar la información.
Finalmente, una vez finalizado el plazo para interponer las reclamaciones y/o recursos administrativos legalmente establecidos, se deberá proceder a la supresión y borrado físico de la información de carácter personal publicada en el sitio Web institucional, en los tablones de anuncios electrónicos, en el canal electrónico o telemático abierto en

Internet, o en la correspondiente Intranet administrativa, referente al procedimiento de concurrencia competitiva.
En otro orden de cosas, en atención al tratamiento de datos de carácter personal realizado por el Órgano consultante, los datos de carácter personal recogidos en el ANEXO ÚNICO y en la documentación que se acompaña a la solicitud deberán archivarse en ficheros previamente declarados por la Consejería de Educación, conforme a lo establecido en la Ley 8/2001, de Protección de Datos de Carácter Personal. Actualmente consta inscrito en el Registro de Ficheros de Datos Personales de esta Agencia, el fichero "AYUDA LIBROS DE TEXTO", con código de Inscripción Nº 2073110001, cuya finalidad declarada es el tratamiento de "Datos de la concesión de ayudas económicas para libros de texto de alumnos matriculados en centros educativos de la Comunidad de Madrid", figurando como responsable del mismo la Viceconsejería de Educación de la Consejería de Educación, que encaja plenamente con la finalidad de los datos recogidos en la Orden objeto del presente Informe.
De lo anterior se extrae que, por parte del Órgano consultante, se ha dado debido cumplimiento a lo dispuesto por el artículo 20 de la LOPD, por el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, y por el artículo 3 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposición general de creación, modificación o supresión de ficheros que contienen datos de carácter personal, habiéndose procedido previamente a la creación, declaración e inscripción del denominado fichero "AYUDA LIBROS DE TEXTO".
Igualmente se señala, que en este caso, y en todos aquellos en que se soliciten datos personales se deberá dar cumplimiento explícito al derecho de información previo al tratamiento de los datos, todo ello de conformidad con lo previsto en el artículo 5 de la LOPD, debiéndose informar de la existencia del fichero, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección del responsable del fichero. En este sentido, y al objeto de cumplir con el deber de información, conforme al artículo 5.1 de la LOPD, en aquellos modelos o solicitudes a través de los cuales se recaben datos de carácter personal deberá aparecer un texto informativo.
El Proyecto de Orden sometido a Informe, acompaña al pie de su ANEXO ÚNICO la correspondiente cláusula informativa que, sin embargo, no resulta plenamente conforme con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, al no indicar todos y cada uno de los extremos a cuya obligatoria mención se refiere el citado precepto.
Así, de acuerdo con el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, los interesados a los que se soliciten datos personales deberán ser informados previamente de modo expreso, preciso e inequívoco de:
- La existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Para ello, y a modo de ejemplo, se podría incluir en los modelos de solicitudes una cláusula como la siguiente:
"Los datos personales recogidos serán incorporados y tratados en el fichero "nombre del fichero", cuya finalidad es la adjudicación de las ayudas de libros de texto y

material didáctico. Dicho fichero, está inscrito en el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid (www.madrid.org/apdcm) y el órgano responsable es "órgano responsable", con domicilio en …… donde el interesado podrá ejercer los derechos de acceso, rectificación o cancelación, todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

Finalmente, tal y como se ha expuesto, el Proyecto de Orden prevé la publicación en lo referente a las listas provisionales de admitidos y excluidos (artículo 10), y en segundo lugar, en lo referente a la resolución de la convocatoria (artículo 12). En ambos casos, la publicación tendrá lugar en los tablones de anuncios de las Direcciones de Área Territorial y en la página Web de la Comunidad de Madrid www.madrid.org. Asimismo, se prevé la resolución de la convocatoria se publicará en el BOCM.

En este sentido, se recomienda que la publicación en los tablones de anuncios de las listas de admitidos y excluidos, así como la resolución de la convocatoria, se ajuste a lo dispuesto en el artículo 14 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, anteriormente transcrito.

A su vez, en el presente caso se pretende la publicación de datos personales que se refieren a la renta per capita de los solicitantes. En este sentido, esta Agencia entiende que dicha información no debe ser objeto de publicación toda vez que la misma podría vulnerar el denominado "principio de calidad de los datos", establecido en el artículo 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de acuerdo con el cual "Los datos de carácter personal sólo se podrán recoger para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

En este sentido, el artículo 6 de la Recomendación 2/2008, de 25 de abril, de la APDCM (Principio de calidad e interés público: normas generales), establece que:

"6.1 En la recogida, tratamiento y publicación de datos de carácter personal en los Boletines y Diarios Oficiales en Internet, en los sitios Web institucionales y canales electrónicos o telemáticos administrativos, tanto si se ha prestado el consentimiento previo del ciudadano afectado como si se trata de uno de los supuestos contemplados por una norma de rango de ley o por una norma comunitaria de aplicación directa, o si la publicación se basa en la existencia de una relación negocial, deberá respetarse el principio de calidad de los datos personales regulado en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

6.2 En todo caso, en el tratamiento de datos de carácter personal realizado mediante la publicación de datos personales tanto en Boletines o Diarios Oficiales a través de Internet, como en sitios Web institucionales y en otros canales electrónicos o telemáticos de las Administraciones públicas y Órganos administrativos a los que se refiere esta Recomendación, el Responsable del tratamiento deberá ponderar todos los derechos e intereses en juego.

Especialmente, dicho Responsable ponderará la posible concurrencia de intereses públicos que justifiquen el acceso a los datos de personas físicas identificadas o identificables, con las exigencias derivadas del derecho fundamental a la protección de datos de carácter personal. Asimismo, deberá ponderar, en cada caso, las exigencias derivadas de los principios de publicidad y objetividad de la Administración pública con las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente con el derecho al honor y a la intimidad personal y familiar de las mismas.

6.3 De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, la publicación de datos personales a través de Boletines o Diarios Oficiales a través de Internet, así como en sitios Web

institucionales y en otros canales electrónicos o telemáticos de las Administraciones públicas y Órganos administrativos, sólo se realizará cuando resulte adecuada, pertinente y no excesiva en relación con el interés público que la justifique.
6.4 La publicación de los datos personales se reputará conforme con la normativa sobre protección de datos cuando la difusión de aquellos a través del medio elegido resulte necesaria en consideración a los hechos y a las circunstancias concurrentes, en aras del interés general, resultando la elección de este tipo de publicación de datos personales la medida más adecuada, pertinente y proporcional de las que puedan adoptarse en orden a la satisfacción del interés público, con cumplimiento de los siguientes requisitos:
a) Que la publicación de los datos personales en dicho medio constituya una medida susceptible de conseguir el objetivo que se pretende (juicio de idoneidad).
b) Que los fines perseguidos con la publicación no puedan alcanzarse de una manera menos intrusiva, teniendo en cuenta la protección de los datos de carácter personal, resultando dicha publicación necesaria por no existir otro medio más moderado para la consecución de tal propósito con igual eficacia (juicio de necesidad).
c) Que la publicación de los datos personales resulte proporcional y equilibrada en atención a la ponderación entre la finalidad perseguida y el grado de restricción del derecho fundamental a la protección de datos de carácter personal, derivando de dicha publicación más beneficios o ventajas para el interés general que perjuicios sobre la protección de los datos de carácter personal (juicio de proporcionalidad en sentido estricto).
6.5 En todo caso, la Administración pública u Órgano administrativo competente deberán optar por realizar dicha publicación a través del sistema o medio de publicidad que suponga un menor nivel de injerencia en el derecho a la intimidad y a la protección de los datos de carácter personal del afectado.
En este sentido, siempre que sea posible, deberá disociarse la información de carácter personal obrante en dichos medios, siguiendo para ello el procedimiento definido por el artículo 3, apartado f) de la Ley Orgánica 15/1999, de 13 de diciembre, de modo que la información que se obtenga no pueda asociarse a personas identificadas o identificables".
Por su parte, el artículo 8 de la citada Recomendación 2/2008, de 25 de abril, de la APDCM (Principio de calidad e interés público: tipología de datos), dispone que:
"8.1 La Administración u Órgano administrativo que inste o realice la publicación se limitará a publicar aquellos datos personales de los afectados que resulten imprescindibles para la finalidad pretendida. En todo caso, deberá evitarse cualquier publicación de datos personales innecesarios para dicha finalidad.
8.2 En la publicación de los datos personales en Boletines o Diarios Oficiales a través de Internet, así como en sitios Web institucionales o en otros canales electrónicos o telemáticos oficiales, el Órgano administrativo competente atenderá especialmente a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.
8.3 Salvo habilitación legal expresa, fundamentada en la existencia de una norma con rango de ley o en una norma comunitaria de aplicación directa que ofrezcan cobertura legal a dicha publicación, se recomienda que no se proceda a la publicación de datos personales en Boletines o Diarios Oficiales a través de Internet, así como en sitios Web institucionales o en otros canales electrónicos o telemáticos administrativos, cuando de la propia naturaleza de los mismos o en atención a su especial nivel de protección dicha publicación resulte claramente incompatible con el respeto a la intimidad, a la dignidad personal o al libre desarrollo de la personalidad.
A dichos efectos, la Administración pública u Órgano administrativo competente deberá considerar la especial protección dispensada por la normativa sobre protección de datos a los siguientes tipos de datos personales:

A) Los de salud, y, de manera específica, los referentes a la discapacidad o invalidez de las personas.
B) Los relativos a la vida sexual y al origen racial de las personas, así como los relacionados con la ideología, la afiliación sindical, la religión o las creencias.
C) Los relacionados con fines policiales o derivados de actos de violencia de género.
D) Los referidos a las personas menores de edad.
E) Los relativos a la comisión de infracciones penales o administrativas.
F) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
G) Los que ofrezcan una definición de las características o de la personalidad de los afectados, así como los que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.
8.4 En estos supuestos, se recomienda que, cuando resulte necesario posibilitar el acceso a través de Internet de datos personales especialmente protegidos, tales como los referidos en el apartado anterior, el Órgano competente adopte las medidas oportunas para que dicho acceso se produzca en relación con los datos mínimos e indispensables para cumplir con la finalidad perseguida.
Asimismo, se recomienda que, cuando se proceda a la publicación de datos especialmente protegidos, el Órgano competente, de acuerdo con lo dispuesto en el artículo 61 de la Ley 30/1992, de 26 de noviembre, proceda -en la medida de lo posible- a la publicación de una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para el conocimiento íntegro de dichos actos y constancia de tal conocimiento.
8.5 En el caso de que se publiquen en los sitios Web institucionales o en otros canales electrónicos o telemáticos oficiales datos personales contenidos en actos administrativos previamente publicados en el Boletín o Diario Oficial correspondiente a través de Internet, la publicación en los referidos sitios deberá limitarse a establecer un enlace o una referencia a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original -por ejemplo, vía RSS-, u otros mecanismos similares, sin necesidad de duplicar la información.
8.6 Cuando la publicación de información en Boletines o Diarios Oficiales a través de Internet, así como en sitios Web o en otros canales electrónicos o telemáticos institucionales, se realice con fines estadísticos o científicos, salvo que concurra el consentimiento del afectado, se recomienda que se evite la publicación de sus datos personales, imposibilitándose la identificación del mismo.
Con carácter general y siempre que sea posible, en este tipo de supuestos deberá disociarse la información de carácter personal obrante en dichos medios, siguiendo para ello el procedimiento definido por el artículo 3, apartado f) de la Ley Orgánica 15/1999, de 13 de diciembre, de modo que la información que se obtenga no pueda asociarse a personas identificadas o identificables".
Por otra parte, según se ha avanzado, el artículo 6.3 del Proyecto de Orden, determina que la presentación de la solicitud implica la autorización para que la Consejería de Educación pueda obtener, a través de la Agencia Estatal de Administración Tributaria, la información necesaria para determinar la renta de la unidad familiar. Se considera que en este supuesto va a existir una cesión de datos de carácter personal, concretamente de carácter tributario, desde la Agencia Estatal de Administración Tributaria a la Consejería de Educación. Si bien en este caso no concurre ninguno de los supuestos del artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, que permitan excepcionar el consentimiento, se considera que la presentación de la solicitud, como bien dice el artículo 7.4 del Proyecto de Orden, lleva consigo el consentimiento de los afectados para que los datos puedan ser cedidos, por lo que se considera conforme al artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre.

¿Cómo debe procederse en la publicación de los datos personales de los alumnos beneficiarios y excluidos en la Convocatoria de ayudas de comedor escolar?

Por la Secretaría General Técnica de la Consejería de Educación de la Comunidad de Madrid se remitió, para su preceptivo informe, el Proyecto de Orden para la concesión de becas de comedor escolar para el curso 2008/2009.
Analizado el Proyecto de Orden se informó lo siguiente:
(…)
El Proyecto de Orden tiene por objeto la aprobación de las bases reguladoras para la concesión de becas de comedor escolar al alumnado escolarizado en Educación Infantil, Educación Primaria y Educación Secundaria Obligatoria en centros sostenidos con fondos públicos o que curse Educación Infantil en centros privados no vinculados a centros de otro nivel educativo, debidamente autorizados en el ámbito de la Comunidad de Madrid. Las becas que se conceden en la modalidad A, lo serán en régimen de concurrencia competitiva. El resto de modalidades serán de concesión directa o concurrencia no competitiva.
Según establece el artículo 4 de la Orden ("Requisitos generales para solicitar beca de comedor escolar"), para solicitar becas de comedor, los alumnos deberán reunir, a la finalización del plazo de presentación de solicitudes los siguientes requisitos:
* Estar empadronados en cualquier municipio de la Comunidad de Madrid.
* Tener plaza de comedor escolar en centro debidamente autorizado.
* Haber presentado las solicitudes y documentación requeridas en la presente Orden en los plazos que se establezcan en la convocatoria anual.
* No estar incurso en alguna de las prohibiciones establecidas en el artículo 13 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.
Según se observa, las BECAS MODALIDAD A se concederán con base en un procedimiento de concurrencia competitiva (capítulo 1 de la Orden), en tanto que las BECAS MODALIDAD B y C (capítulos 2 y 3), así como las concedidas CON CARÁCTER EXCEPCIONAL (capítulo 4) y las otorgada a consecuencia de circunstancias de URGENCIA SOCIAL Y PARA MENORES EN SITUACIÓN DE ACOGIMIENTO RESIDENCIAL O FAMILIAR (capítulo 5), y PARA ALUMNOS CUYAS FAMILIAS HAYAN SIDO VÍCITIMAS DEL TERRORISMO (capítulo 6), se adjudicarán a través de un procedimiento de concesión directa.
Con independencia de los supuestos en los que no resulte aplicable el procedimiento de concurrencia competitiva, en cuanto a los requisitos exigibles para la MODALIDAD A, se establece "que la renta per cápita anual de la unidad familiar no supere los umbrales máximos que se exijan en cada convocatoria" (artículo 7), entendiéndose a dichos efectos "por renta per cápita familiar los ingresos familiares divididos entre el número de miembros de la unidad familiar" (artículo 8). De otra parte, para la determinación de la unidad familiar, en el artículo 9 de la Orden se establecen determinados criterios en función de las diferentes situaciones personales y/o familiares de los solicitantes. En orden a su necesaria justificación, el Órgano responsable procederá a recabar de los solicitantes diferente documentación acreditativa de dichas situaciones.
Las solicitudes deberán cumplimentarse en los modelos correspondientes que se acompañan como ANEXOS de la Orden, en sus diversas modalidades A, B, C, de carácter excepcional, y destinada a alumnos cuyas familias hayan sido víctimas del terrorismo o a menores en situación de acogimiento familiar. Con la presentación de la solicitud, deberán acompañarse diversos documentos que contienen datos de carácter personal. En concreto, en relación con la MODALIDAD A, dicha solicitud deberá acompañarse -entre otros documentos- de fotocopia cotejada de:
- DNI o NIE (o pasaporte en su caso).

- Libro de Familia y, en su caso, Título de familia númerosa.
- Certificados sobre discapacidad física, psíquica o sensorial.
- Para el cálculo de la renta per cápita de cada unidad familiar, la Consejería de Educación de la Comunidad de Madrid recabará de la Agencia Estatal de Administración Tributaria, la información relativa a la renta anual del ejercicio correspondiente a todos los miembros de la unidad familiar.

De este modo, como queda expuesto, la solicitud implica la autorización para que la Consejería de Educación pueda obtener, a través de la Agencia Estatal de la Administración Tributaria la información necesaria para determinar la renta de la unidad familiar.

Actualmente, consta inscrito en el Registro de Ficheros de Datos Personales de esta Agencia, el fichero denominado "AYUDAS DE COMEDOR", con código de Inscripción Nº 2060130002, cuya finalidad declarada es "El procesamiento de los datos contenidos en el fichero de solicitudes de ayudas de comedor escolar para valorar la concesión o denegación de dicha ayuda", figurando como responsable del mismo la Viceconsejería de Educación de la Consejería de Educación.

De lo anterior se extrae que, por parte del Órgano consultante, se ha dado debido cumplimiento a lo dispuesto por el artículo 20 de la LOPD, por el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, y por el artículo 3 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposición general de creación, modificación o supresión de ficheros que contienen datos de carácter personal, habiéndose procedido previamente a la creación, declaración e inscripción del denominado fichero "AYUDAS DE COMEDOR".

Igualmente se señala, que en este caso, y en todos aquellos en que se soliciten datos personales se deberá dar cumplimiento explícito al derecho de información previo al tratamiento de los datos, todo ello de conformidad con lo previsto en el artículo 5 de la LOPD, debiéndose informar de la existencia del fichero, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección del responsable del fichero. En este sentido, y al objeto de cumplir con el deber de información, conforme al artículo 5.1 de la LOPD, en aquellos modelos o solicitudes a través de los cuales se recaben datos de carácter personal deberá aparecer un texto informativo.

En el presente caso, según se aprecia, en los ANEXOS IV y V, relativos a la SOLICITUD DE BECA PARA COMEDOR ESCOLAR "MODALIDAD C" y "MODALIDAD D", del proyecto de Orden, a través de los cuales se procede a la recogida de datos de carácter personal, se ha incorporado la correspondiente cláusula que resulta plenamente conforme con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, cumpliendo con lo establecido por dicho precepto.

Sin embargo, en lo que se refiere a los modelos ANEXOS II, III y VI, referidos a la SOLICITUD DE BECA PARA COMEDOR ESCOLAR "MODALIDAD A", "MODALIDAD B", y "Destinadas a alumnos cuyas familias hayan sido víctimas del terrorismo y a menores en situación de acogimiento familiar", no se ha procedido a la incorporación de la referida cláusula.

En consecuencia, por parte del Órgano consultante, deberá procederse a la inclusión en dichos modelos de una cláusula informativa similar a la contenida en los ANEXOS IV y V de las MODALIDADES "C" y "D".

De otra parte, en relación con la "MODALIDAD A", de acuerdo con lo dispuesto en los artículos 16 y 19 de la Orden se procederá, respectivamente, a la elaboración de las relaciones provisionales de concesión o denegación de las solicitudes de becas de comedor, que se expondrán en los tablones de anuncios de los centros educativos, y al dictado de la resolución definitiva de la convocatoria, con indicación de la relación definitiva de beneficiarios y de las cuantías de las becas, así como de las solicitudes

denegadas y del motivo de dicha denegación, que se hará pública en los tablones de anuncios de los centros educativos y en la página Web www.madrid.org.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, de acuerdo con la normativa administrativa aplicable, este tipo de procedimientos han de reputarse como procedimientos de concurrencia competitiva, toda vez que existiendo una pluralidad de solicitantes y un número de plazas o de créditos limitados, debe procederse a la asignación de los mismos en función de la consideración de unos méritos o requisitos susceptibles de cómputo o valoración.
Siguiendo lo previsto en el artículo 14.2 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Webs institucionales y en otros medios electrónicos y telemáticos, "La publicación de datos personales en Boletines o Diarios Oficiales en Internet derivada de los procedimientos de concurrencia competitiva se fundamenta en el artículo 59.6. b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".
En estos casos, el órgano administrativo titular de la competencia administrativa del procedimiento de concurrencia competitiva correspondiente, deberá decidir sobre los datos personales que sean objeto de publicación con acceso no identificado por cualquier persona, debiendo producir dicha publicación la menor injerencia posible sobre el derecho a la intimidad y a la protección de los datos de carácter personal de los ciudadanos afectados.
En este tipo de supuestos, se recomienda que el acceso no identificado por cualquier persona, realizado como consecuencia de la publicación de datos personales en Boletines y Diarios Oficiales en Internet, se limite a los datos personales mínimos correspondientes al resultado final del procedimiento administrativo, a la indicación de los datos personales mínimos de los beneficiarios o adjudicatarios de dicho procedimiento, así como -en su caso- a la publicación de la baremación total de los méritos valorados.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, se cumple así suficientemente con las exigencias derivadas de lo dispuesto en el artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, causando esta publicación una menor injerencia en la intimidad de los ciudadanos afectados por el tratamiento de sus datos.
A su vez, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación de actos administrativos de trámite referentes a procedimientos de concurrencia competitiva en Boletines o Diarios Oficiales en Internet o en sitios Web institucionales sea sustituida por la utilización de un espacio privado, con acceso restringido, en los sitios Web institucionales.
Así, por ejemplo -entre otros datos de carácter personal contenidos en los actos administrativos de trámite-, cuando los procedimientos de concurrencia competitiva incorporen algún trámite administrativo consistente en la realización de una baremación parcial de los méritos de los ciudadanos afectados, se recomienda que se proceda a la publicación de los resultados de la baremación parcial a través de este espacio privado, con acceso restringido, en los sitios Web institucionales, en el canal electrónico o telemático abierto en Internet, en los tablones de anuncios electrónicos, o, en su caso, en la correspondiente Intranet administrativa.
La utilización de estos espacios privados garantizará que los participantes en dichos procedimientos puedan conocer los actos administrativos derivados de la tramitación del expediente identificándose mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios como

el uso de un nombre de usuario y una contraseña segura, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
Para la publicación en los sitios Web institucionales, sin restricción ni identificación de acceso, de actos administrativos de trámite derivados de procedimientos de concurrencia competitiva que contengan datos de carácter personal de los ciudadanos afectados, se recomienda que el Órgano competente obtenga el consentimiento previo y expreso de los mismos.
De acuerdo con lo indicado anteriormente, en caso de no obtenerse este consentimiento, se recomienda que la publicación de dichos actos administrativos de trámite se realice únicamente en espacios privados de los tablones de anuncios electrónicos, del sitio Web institucional, o del canal electrónico o telemático abierto en Internet, o, en su caso, en la correspondiente Intranet administrativa, exigiéndose la acreditación indubitada de la identidad de la persona que acceda a los datos mediante el uso de cualquiera de los medios de identificación señalados en los apartados anteriores.
Especialmente, cuando los procedimientos de concurrencia competitiva incorporen algún dato de carácter personal relativo a la existencia de discapacidades físicas, psíquicas o sensoriales de los afectados, se recomienda que se proceda únicamente a la publicación de los resultados mínimos correspondientes a la baremación efectuada.
En estos supuestos, se recomienda que, de acuerdo con lo dispuesto en el artículo 61 de la Ley 30/1992, de 26 de noviembre, por parte de la Administración pública u Órgano administrativo competente, se proceda -en la medida de lo posible- a la publicación de una somera indicación del contenido de dicha baremación y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para el conocimiento íntegro de la misma y constancia de tal conocimiento.
En el caso de que se publiquen en los sitios Web institucionales datos relativos a actos administrativos de procedimientos de concurrencia competitiva que a su vez hayan sido publicados en el Boletín o Diario Oficial correspondiente a través de Internet, la publicación en los referidos sitios deberá limitarse a establecer una referencia o enlace a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original - por ejemplo, vía RSS -, u otros mecanismos similares, sin necesidad de duplicar la información.
Finalmente, una vez finalizado el plazo para interponer las reclamaciones y/o recursos administrativos legalmente establecidos, se deberá proceder a la supresión y borrado físico de la información de carácter personal publicada en el sitio Web institucional, en los tablones de anuncios electrónicos, en el canal electrónico o telemático abierto en Internet, o en la correspondiente Intranet administrativa, referente al procedimiento de concurrencia competitiva.
En consecuencia, una vez cumplida la finalidad de notificación debería procederse a la cancelación de los datos definitivos publicados en la página Web www.madrid.org y en los tablones de anuncios, proponiéndose -a su vez- como "mejor práctica" que dicha obligación se prevea en la propia Orden objeto del presente Informe.
De otra parte, en relación con la publicación de los "listados provisionales de concesión y denegación de solicitudes de becas", se recomienda que la publicación en los tablones de anuncios de las listas de admitidos y excluidos, así como la resolución de la convocatoria, se ajuste a lo dispuesto en el artículo 14 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, anteriormente transcrito.
A su vez, también en el presente caso el órgano consultante deberá estar a lo establecido en el artículo 4.1 de la Ley Orgánica 15/1999, de 13 de diciembre (principio de calidad), de acuerdo con el cual "Los datos de carácter personal sólo se podrán recoger para su tratamiento, cuando sean adecuados, pertinentes y no

excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".
En este sentido, del mismo modo que se expuso en la pregunta anterior, se recomienda que la actuación del órgano administrativo se ajuste a lo dispuesto en los artículos 6 y 8 de la Recomendación 2/2008, de 25 de abril, sobre Publicación de Datos Personales en Boletines y Diarios Oficales en Internet, en sitios Web institucionales y en otros medios electrónicos y telemáticos.
Asimismo, deberá tenerse en cuenta que, de acuerdo con el artículo 7 de dicha Recomendación (Principio de calidad e interés público: nivel de publicidad):
"7.2 En los supuestos en los que rija el principio de publicidad, se reputará plenamente conforme con la normativa sobre protección de datos el acceso de los interesados en el procedimiento administrativo a los datos de carácter personal relacionados con el mismo y publicados por la Administración pública u Órgano administrativo competente en un sitio Web institucional o en otros canales electrónicos o telemáticos, siempre que requiera como requisito indispensable de la identificación y autenticación del ciudadano que lo realice, mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios, como la introducción de una clave de acceso personalizada previamente asignada por la Administración, con su correspondiente contraseña, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
En este supuesto el acceso podrá realizarse tanto a través de un área restringida ubicada en el sitio Web institucional o en el canal electrónico o telemático abierto en Internet, como -en su caso- a través de la utilización de una Intranet administrativa que requiera la identificación y autenticación por mecanismos fiables que permitan acreditar indubitadamente la identidad de la persona mediante el uso de cualquiera de los medios de identificación señalados.
7.3 De acuerdo con el artículo 12 (Publicación electrónica del tablón de anuncios o edictos) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos podrá ser sustituida o complementada por su publicación en la sede electrónica del organismo correspondiente.
En consecuencia, en su caso, el acceso a los tablones de anuncios electrónicos deberá verificarse a través de la consulta identificada del interesado, utilizando para ello cualquiera de los medios identificativos a los que se refieren los apartados anteriores.
También en este supuesto, el acceso a los tablones de anuncios electrónicos podrá realizarse tanto a través de un área restringida ubicada en el sitio Web institucional o en el canal electrónico o telemático abierto en Internet, como -en su caso- a través de la utilización de una Intranet administrativa.
7.4 La publicación de datos de carácter personal en Boletines o Diarios Oficiales a través de Internet supone un mayor nivel de injerencia sobre el derecho fundamental a la protección de datos de carácter personal que la publicación de los mismos a través de sitios Web institucionales, o de cualquier otro medio electrónico o telemático administrativo, al constituir dichos Boletines o Diarios oficiales "fuentes accesibles al público", de acuerdo con la definición de las mismas contenida en el artículo 3, apartado j) de la Ley Orgánica 15/1999, de 13 de diciembre.
En consecuencia, se recomienda que dicha publicación en Boletines o Diarios oficiales, y, en consecuencia, el acceso no identificado de cualquier ciudadano a los datos así publicados, se produzca únicamente en aquellos supuestos en que se trate de uno de los supuestos contemplados por una norma con rango de ley o por una norma comunitaria de aplicación directa.

7.5 La publicación no restringida de datos de carácter personal, con acceso no identificado y universal, de datos de carácter personal en sitios Web institucionales, o en cualquier otro medio electrónico o telemático administrativo, supone un menor nivel de injerencia sobre el derecho fundamental a la protección de datos de carácter personal que la publicación de dichos datos personales en Boletines y Diarios oficiales. En consecuencia, se recomienda que, siempre que una norma con rango de ley o una norma comunitaria de aplicación directa no establezcan lo contrario, la Administración pública u Órgano administrativo competente que deba proceder a la publicación no restringida de datos de carácter personal que posibilite el acceso no identificado y universal a los mismos, lo realice a través de un sitio Web institucional o mediante cualquier otro medio electrónico o telemático, sin acudir a la publicación de los datos a través de Boletines o Diarios oficiales.
Para el mejor cumplimiento de esta recomendación, se aconseja que en la Orden o Resolución correspondiente se señale el medio a través del cual se llevará a cabo la publicación de los datos personales en el sitio Web institucional de la Administración u Órgano administrativo competente, o en el tablón de anuncios electrónico.
7.6 En todo caso, se recomienda que en la Orden, u otra Disposición de carácter general, en la que establezca la publicidad de los datos personales derivados del procedimiento administrativo correspondiente, se indique -de manera concreta y específica- el medio de publicación elegido por el Órgano competente para la consecución de los correspondientes efectos jurídicos perseguidos con dicha publicación".
En otro orden de cosas, según se ha avanzado, el Proyecto de Orden determina que la presentación de la solicitud implica la autorización para que la Consejería de Educación pueda obtener, a través de la Agencia Estatal de Administración Tributaria, la información necesaria para determinar la renta de la unidad familiar. Se considera que en este supuesto va a existir una cesión de datos de carácter personal, concretamente de carácter tributario, desde la Agencia Estatal de Administración Tributaria a la Consejería de Educación. Si bien en este caso no concurre ninguno de los supuestos del artículo 11.2 de la Ley Orgánica 15/1999, de 13 de diciembre, que permitan excepcionar el consentimiento, se considera que la presentación de la solicitud (artículo 11 del Proyecto de Orden) llevaría consigo el consentimiento de los afectados para que los datos puedan ser cedidos, por lo que se considera conforme al artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre.
¿Cómo debe procederse en la publicación de los datos personales de los alumnos con aprovechamiento excelente para cursar estudios en las Universidades de la Comunidad de Madrid?
Por la Secretaría General Técnica de la Consejería de Educación de la Comunidad de Madrid se remitió, para su preceptivo informe, el Proyecto de Orden para la concesión de ayudas al estudio a los alumnos con aprovechamiento académico excelente para cursar estudios en las Universidades de la Comunidad de Madrid, sus Centros adscritos y el Centro Asociado de la UNED en Madrid, correspondientes al curso 2008-2009.
Analizado el Proyecto de Orden se informó lo siguiente:
(…)
El Proyecto de Orden tiene por finalidad "estimular y apoyar la formación de alumnos universitarios de aprovechamiento académico excelente. A este fin, la Consejería de Educación ha puesto en marcha este programa de becas mediante el que se facilita la colaboración de estos alumnos con profesores universitarios de reconocida ejecutoria en el campo de la investigación, con el evidente beneficio que tal colaboración entraña. Alternativamente, se prevé que los estudiantes puedan participar en tareas de apoyo a los profesores universitarios". Las correspondientes becas se convocan en régimen de concurrencia competitiva, encontrándose destinadas a aquellos alumnos con

aprovechamiento académico excelente, en las condiciones que se establecen en la propia orden.
También a juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, de acuerdo con la normativa administrativa aplicable, este tipo de procedimientos han de reputarse como procedimientos de concurrencia competitiva, toda vez que existiendo una pluralidad de solicitantes y un número de plazas o de créditos limitados, debe procederse a la asignación de los mismos en función de la consideración de unos méritos o requisitos susceptibles de cómputo o valoración.
Siguiendo lo previsto en el artículo 14.2 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios Webs institucionales y en otros medios electrónicos y telemáticos, "La publicación de datos personales en Boletines o Diarios Oficiales en Internet derivada de los procedimientos de concurrencia competitiva se fundamenta en el artículo 59.6. b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".
En estos casos, el órgano administrativo titular de la competencia administrativa del procedimiento de concurrencia competitiva correspondiente, deberá decidir sobre los datos personales que sean objeto de publicación con acceso no identificado por cualquier persona, debiendo producir dicha publicación la menor injerencia posible sobre el derecho a la intimidad y a la protección de los datos de carácter personal de los ciudadanos afectados.
En este tipo de supuestos, se recomienda que el acceso no identificado por cualquier persona, realizado como consecuencia de la publicación de datos personales en Boletines y Diarios Oficiales en Internet, se limite a los datos personales mínimos correspondientes al resultado final del procedimiento administrativo, a la indicación de los datos personales mínimos de los beneficiarios o adjudicatarios de dicho procedimiento, así como -en su caso- a la publicación de la baremación total de los méritos valorados.
A juicio de la Agencia de Protección de Datos de la Comunidad de Madrid, se cumple así suficientemente con las exigencias derivadas de lo dispuesto en el artículo 59.6 b) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, causando esta publicación una menor injerencia en la intimidad de los ciudadanos afectados por el tratamiento de sus datos.
A su vez, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda que la publicación de actos administrativos de trámite referentes a procedimientos de concurrencia competitiva en Boletines o Diarios Oficiales en Internet o en sitios Web institucionales sea sustituida por la utilización de un espacio privado, con acceso restringido, en los sitios Web institucionales.
Así, por ejemplo -entre otros datos de carácter personal contenidos en los actos administrativos de trámite-, cuando los procedimientos de concurrencia competitiva incorporen algún trámite administrativo consistente en la realización de una baremación parcial de los méritos de los ciudadanos afectados, se recomienda que se proceda a la publicación de los resultados de la baremación parcial a través de este espacio privado, con acceso restringido, en los sitios Web institucionales, en el canal electrónico o telemático abierto en Internet, en los tablones de anuncios electrónicos, o, en su caso, en la correspondiente Intranet administrativa.
La utilización de estos espacios privados garantizará que los participantes en dichos procedimientos puedan conocer los actos administrativos derivados de la tramitación del expediente identificándose mediante sistemas de firma electrónica avanzada, incluyendo los incorporados al Documento Nacional de Identidad, u otros medios como

el uso de un nombre de usuario y una contraseña segura, la aportación de información sólo conocida por ambas partes, o mecanismos equivalentes.
Para la publicación en los sitios Web institucionales, sin restricción ni identificación de acceso, de actos administrativos de trámite derivados de procedimientos de concurrencia competitiva que contengan datos de carácter personal de los ciudadanos afectados, se recomienda que el Órgano competente obtenga el consentimiento previo y expreso de los mismos.
De acuerdo con lo indicado anteriormente, en caso de no obtenerse este consentimiento, se recomienda que la publicación de dichos actos administrativos de trámite se realice únicamente en espacios privados de los tablones de anuncios electrónicos, del sitio Web institucional, o del canal electrónico o telemático abierto en Internet, o, en su caso, en la correspondiente Intranet administrativa, exigiéndose la acreditación indubitada de la identidad de la persona que acceda a los datos mediante el uso de cualquiera de los medios de identificación señalados en los apartados anteriores.
Especialmente, cuando los procedimientos de concurrencia competitiva incorporen algún dato de carácter personal relativo a la existencia de discapacidades físicas, psíquicas o sensoriales de los afectados, se recomienda que se proceda únicamente a la publicación de los resultados mínimos correspondientes a la baremación efectuada.
En estos supuestos, se recomienda que, de acuerdo con lo dispuesto en el artículo 61 de la Ley 30/1992, de 26 de noviembre, por parte de la Administración pública u Órgano administrativo competente, se proceda -en la medida de lo posible- a la publicación de una somera indicación del contenido de dicha baremación y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para el conocimiento íntegro de la misma y constancia de tal conocimiento.
En el caso de que se publiquen en los sitios Web institucionales datos relativos a actos administrativos de procedimientos de concurrencia competitiva que a su vez hayan sido publicados en el Boletín o Diario Oficial correspondiente a través de Internet, la publicación en los referidos sitios deberá limitarse a establecer una referencia o enlace a dichos Boletines o Diarios Oficiales en Internet, redifusión o sindicación de su contenido electrónico original - por ejemplo, vía RSS -, u otros mecanismos similares, sin necesidad de duplicar la información.
Finalmente, una vez finalizado el plazo para interponer las reclamaciones y/o recursos administrativos legalmente establecidos, se deberá proceder a la supresión y borrado físico de la información de carácter personal publicada en el sitio Web institucional, en los tablones de anuncios electrónicos, en el canal electrónico o telemático abierto en Internet, o en la correspondiente Intranet administrativa, referente al procedimiento de concurrencia competitiva.
De otra parte, los requisitos de los solicitantes se establecen en los artículos 5 y 6 de la Orden, disponiéndose en los artículos 7 y 8 de la misma las normas relativas a la "Nota media" mínima necesaria para solicitar las ayudas, y las relativas al "Cálculo de (dicha) nota media".
Según establecen los artículos 9 y 10 del proyecto de Orden, relativos -respectivamente- a los "Requisitos de las solicitudes" y a la "Documentación a aportar", la solicitud contenida en el ANEXO I de la convocatoria deberá acompañarse -a su vez- de diversos documentos, entre los que se encuentran:
* Una declaración, positiva o negativa, de otras ayudas y subvenciones al estudio solicitadas durante el curso anterior al que se proponen las ayudas.
* Una declaración de la nota media de las calificaciones obtenidas en el último curso realizado, calculada con dos decimales.
* Una declaración del número de matrículas de honor obtenidas en el último curso.
* Una fotocopia del DNI-NIF o fotocopia del pasaporte o tarjeta de residencia así como un teléfono de contacto.

* Una declaración jurada, según ANEXO VII, de no encontrarse incurso en los supuestos establecidos en el artículo 13 de la Ley 38/2003, General de Subvenciones.
* La presentación de la solicitud de la beca implicará la autorización a las administraciones educativas de la Comunidad de Madrid para obtener los datos necesarios para determinar las obligaciones tributarias y de la Seguridad Social a efectos de beca a través de las correspondientes administraciones.

Según queda expuesto, las solicitudes deberán cumplimentarse en el modelo correspondiente que se acompaña como ANEXO I de la Orden. La presentación de la solicitud implica la autorización para que la Consejería de Educación pueda obtener los datos necesarios para determinar las obligaciones tributarias y de Seguridad Social a efectos de beca a través de las correspondientes administraciones.

Actualmente consta inscrito en el Registro de Ficheros de Datos Personales de esta Agencia, el fichero denominado "EXCELYERAS", con código de Inscripción Nº 1973170170, cuya finalidad declarada es "LA GESTION DE TODAS LAS BECAS SOLICITADAS Y CONCEDIDAS A LOS ALUMNOS EXCELENTES Y ERASMUS, POR LA DIRECCION GENERAL DE UNIVERSIDADES, ASÍ COMO LA EMISION DE COMUNICACIONES DE INTERÉS", figurando como responsable del mismo la Dirección General de Universidades e Investigación.

De lo anterior se extrae que, por parte del Órgano consultante, se ha dado debido cumplimiento a lo dispuesto por el artículo 20 de la LOPD, por el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid, y por el artículo 3 del Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposición general de creación, modificación o supresión de ficheros que contienen datos de carácter personal, habiéndose procedido previamente a la creación, declaración e inscripción del denominado fichero "EXCELYERAS".

Igualmente se señala, que en este caso, y en todos aquellos en que se soliciten datos personales se deberá dar cumplimiento explícito al derecho de información previo al tratamiento de los datos, todo ello de conformidad con lo previsto en el artículo 5 de la LOPD, debiéndose informar de la existencia del fichero, de la finalidad de la recogida de los datos, de los destinatarios de la información y de la identidad y dirección del responsable del fichero. En este sentido, y al objeto de cumplir con el deber de información, conforme al artículo 5.1 de la LOPD, en aquellos modelos o solicitudes a través de los cuales se recaben datos de carácter personal deberá aparecer un texto informativo.

En el presente caso, según se aprecia, en los ANEXOS I, II, III, IV, V, VI y VII del proyecto de Orden, a través de los cuales se procede a la recogida de datos de carácter personal, se ha incorporado la correspondiente cláusula que resulta plenamente conforme con lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, cumpliendo con lo establecido por dicho precepto.

De otra parte, de acuerdo con lo dispuesto en los artículos 13 y 16 de la Orden se procederá, respectivamente, a la elaboración y publicación de una resolución provisional de alumnos beneficiarios, que deberá publicarse en los tablones anuncios de la Consejería de Educación y de la Universidad respectiva, y estarán a disposición de los interesados en el Centro de Información y Asesoramiento Universitario de la Comunidad de Madrid, y al dictado de la resolución definitiva de la Orden de convocatoria, con indicación de la el nombre y apellidos de los beneficiarios, su NIF y la cuantía de la ayuda. Asimismo, se publicará una lista de alumnos suplentes ordenados conforme a los criterios expuestos en el artículo 15 de la Orden ("Baremación de méritos"). Dicha resolución definitiva se hará pública en los tablones de anuncios de la Consejería de Educación y estarán a disposición de los interesados en el Centro de Información y Asesoramiento Universitario de la Comunidad de Madrid y en la página Web www.emes.es.

En este sentido, se recomienda que la publicación en los tablones de anuncios de las listas de admitidos y excluidos, así como la resolución de la convocatoria, se ajuste a lo dispuesto en el artículo 14 de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, anteriormente transcrito.
De este modo, una vez cumplida la finalidad de notificación debería procederse a la cancelación de los datos definitivos publicados en la página Web www.emes.es y en los tablones de anuncios, proponiéndose -a su vez- como "mejor práctica" que dicha obligación se prevea en la propia Orden.
De esta forma, cuando finalice el plazo de reclamaciones de diez días en relación con los listados provisionales de beneficiarios de las ayudas, los datos de carácter personal publicados deberían ser retirados de los correspondientes "tablones de anuncios" de los Órganos competentes y/o -en su caso- deberían ser borrados de Internet, procediéndose a la cancelación de los mismos, puesto que según prevé el artículo 4.5 de la LOPD, los datos de carácter personal deben ser cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados, finalidad que en este caso no es otra, según se reitera, que la publicación a efectos de notificación.
En resumen, transcurrido el plazo fijado de diez días establecido en el artículo 13 de la Orden para que los interesados puedan realizar "alegaciones", haciendo uso -en su caso- de dicho plazo, deberá procederse a la cancelación de los datos, mediante el bloqueo de dichos datos, procediendo a la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para las finalidades previstas por la legislación aplicable. En consecuencia, en la Orden objeto de este informe se recomienda como "mejor práctica" que se prevea la cancelación de los datos personales una vez finalizado el plazo al que se ha hecho mención.
Finalmente, también en este supuesto deberán tenerse en cuenta las previsiones contenidas en los artículos 6, 7 y 8, (principio de calidad) de la Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid.
(…).

¿Debe un Centro Educativo de la Comunidad de Madrid entregar copia de un expediente al Defensor del Pueblo cuando esta institución lo demande? ¿Y al Defensor del Menor?

La comunicación de datos al Defensor del Pueblo, constituye uno de los supuestos específicamente recogidos por la LOPD. De acuerdo con lo dispuesto en el artículo 11.2 d) de dicha Ley Orgánica, la respuesta es sí, debiendo realizarse dicha comunicación de datos con la diligencia necesaria de custodia en orden a proteger el derecho fundamental a la protección de datos.
Respecto a la solicitud de datos de carácter personal por parte del Defensor del Menor, hay que analizar cuales son las competencias que atribuye al Defensor del Menor la Ley 5/1996, de 8 de julio, para saber si existe alguna excepción legal al límite del consentimiento para la cesión de datos de carácter personal.
Así, el artículo 3.1. a) de la citada Ley 5/1996, de 8 de julio, atribuye al Defensor del Menor de la Comunidad de Madrid la competencia para supervisar la acción de las Administraciones Públicas de la Comunidad de Madrid, y de cuantas entidades privadas presten servicios a la infancia y la adolescencia en la Comunidad, para verificar el respeto a sus derechos y orientar sus actuaciones en pro de la defensa de los mismos, dando posterior cuenta a la Asamblea.
Asimismo, el artículo 20.1 de dicha Ley establece la obligación de que todos los poderes públicos, así como cualquiera de las entidades privadas, que presten servicios a los menores y que reciban financiación pública, están obligados a auxiliar

con carácter preferente y urgente al Defensor del Menor, en sus investigaciones e inspecciones.
Por lo tanto, los preceptos aludidos suponen la existencia de la habilitación legal necesaria para que se puedan entregar al Defensor del Menor los expedientes con datos de carácter personal que el mismo solicite, siempre y cuando sea para la finalidad de defensa de los intereses de los menores, y teniendo en cuenta que para su traslado se deberá observar la diligencia necesaria de custodia en orden a proteger el derecho fundamental a la protección de datos de los menores.

¿Se puede facilitar por parte del un Organismo Autónomo la documentación de los expedientes completos de las subvenciones que le han sido solicitadas a un diputado de la Asamblea de Madrid?

Para valorar si la información solicitada por un diputado de un Grupo Parlamentario a través de la Mesa de la Asamblea de Madrid se puede comunicar sin el consentimiento previo de los afectados se ha de analizar si esta cesión se encuentra recogida en alguna norma de rango legal, y si está orientada al cumplimiento de un fin legítimo entre cedente y cesionario, tal y como establece el artículo 11 de la LOPD.
Sobre este particular hay que señalar que los diputados de la Asamblea de Madrid tienen la función de control del Consejo de Gobierno de la Comunidad Autónoma. A estos efectos el Estatuto de Autonomía de la Comunidad de Madrid, aprobado por la Ley Orgánica 3/1983, de 25 de febrero, establece en su el artículo 14.3 que una de las funciones de la Asamblea es el control de la acción del Consejo de Gobierno. La forma de instar y de realizar dicho control ha sido objeto de desarrollo a través del artículo 18 del Reglamento, de 30 de enero de 1997, de la Asamblea Legislativa de la Comunidad de Madrid, en el que se dispone que para el mejor cumplimiento de sus funciones parlamentarias, los Diputados, con el visto bueno del Portavoz del respectivo Grupo Parlamentario, tendrán derecho a solicitar del Consejo de Gobierno los datos, informes o documentos que en obren en poder de éste como consecuencia de actuaciones administrativas realizadas por la Administración Pública de la Comunidad de Madrid. La solicitud se dirigirá en todo caso por conducto del Presidente.
Por lo tanto, el Organismo Autónomo podrá ceder la información solicitada, no siendo preciso en este caso solicitar el consentimiento de las personas afectadas, puesto que la cesión estaría autorizada por ley, en concreto, por el artículo 14.3 del Estatuto de Autonomía de la Comunidad de Madrid, siempre y cuando la finalidad de la cesión sea el control de la acción del Consejo de Gobierno, conforme al citado precepto.

¿Puede intercambiarse información entre los Equipos de Orientación Educativos y los Equipos de Salud Mental?

Con carácter general, sólo podrá procederse a dicho intercambio de información si lo dispone una norma con rango de Ley o si se va a solicitar con carácter previo el consentimiento informado del padre, madre o tutor del menor. Únicamente en estos casos se cumpliría con lo dispuesto en los artículos 6 y 11 de la LOPD para la recogida, tratamiento y cesión de los datos de carácter personal.
Ello no obstante, debe tenerse en cuenta lo dispuesto en el artículo 7.6 de la propia LOPD, en donde -en relación con los datos especialmente protegidos (entre los que se encuentran los relativos a la salud de las personas)- se establece que "(…) podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo (en donde se incluyen los relativos al origen racial, salud y vida sexual), cuando dicho tratamiento resulte necesario para la prevención o para el diagnósticos médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por

un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto". "También podrán ser objeto de tratamiento (dichos datos) cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".
En consecuencia, en aplicación de dicho precepto, resultará conforme con la LOPD la comunicación de "datos de salud" (por ejemplo relativos a la "salud mental" de los afectados) a favor de los "Equipos de Salud Mental" cuando dicha cesión reúna los requisitos establecidos en el citado artículo 7.6 de la LOPD.
Por otra parte, en la medida en que los datos personales recogidos en los cuestionarios utilizados para solicitar el consentimiento informado de los padres/tutores se incorporen a un fichero informatizado o manual estructurado, los mismos deberán contener la leyenda informativa correspondiente relativa al cumplimiento del artículo 5 LOPD.

¿Pueden cederse por el Instituto Madrileños del Menor y la Familia datos de personas que habían pertenecido al Sistema de Protección de la Comunidad de Madrid a la Consejería de Educación para la realización de una investigación?

Sí, porque la cesión se ha efectúa entre administraciones públicas y tiene como objeto la realización de una investigación, no siendo necesario el consentimiento de los afectados (art. 11.2.e LOPD). No obstante, la APDCM considera que en estos supuestos los datos de carácter personal deben ser cedidos de forma disociada, es decir, de manera que el tratamiento de datos personales se haga de forma que no pueda asociarse a persona identificada o identificable.
Además, con carácter previo al tratamiento de los datos por el cesionario, y de conformidad con el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, al cederse la información con datos personales se debe de haber procedido a la aprobación de la correspondiente disposición general de creación del fichero.
Asimismo, y en lo referente a los colaboradores externos de la Comunidad de Madrid, éstos deben firmar alguna cláusula de confidencialidad.
La APDCM recomienda que no se proceda a la publicación del estudio de investigación en la medida de que en el mismo aparezcan datos de carácter personal. En general, para los proyectos de investigación resulta recomendable que la información se ceda o utilice siempre de forma disociada.
Además, finalizada la investigación, los datos personales cedidos a la Consejería de Educación, deben ser cancelados por la misma puesto que han cumplido la finalidad para la cual fueron solicitados.

¿Es conforme a la LOPD la solicitud por parte de la Concejalía de Educación de un Ayuntamiento a una Escuela Infantil del Municipio de una relación de familias pertenecientes a dicha Escuela, así como su domicilio postal, para presentar el Programa denominado "AMPLÍA"?

En relación con esta pregunta, debe tenerse en cuenta que la Concejalía de Educación del Ayuntamiento ejerce las competencias que atribuye al municipio en materia de educación el artículo 25.2.n) de la Ley 7/1985, de 2 de abril, de Bases del Régimen Local, es decir, la competencia para participar en la programación de la enseñanza y cooperar con la Administración educativa en la creación, construcción y sostenimiento de los centros públicos docentes.
Por su parte, la Escuela Infantil forma parte de la Red Pública de Centros de Educación Infantil de la Comunidad de Madrid, tratándose de un Centro en donde se desarrolla la primera etapa del sistema educativo (Educación Infantil).
En consecuencia, se considera que tanto la Concejalía de Educación del Ayuntamiento como la Escuela Infantil desarrollan una serie de actuaciones sobre una misma materia, como es la materia educativa, por lo que la cesión de datos de carácter personal por la Escuela Infantil a la Concejalía sería conforme con lo previsto en el artículo 21.1 de la LOPD.

¿Resulta conforme con lo dispuesto en la normativa sobre protección de datos la utilización por parte de los alumnos de un Centro Educativo de una plataforma de Internet para realizar cursos on-line?

De acuerdo con la consulta, la participación en dichos cursos requiere, como herramienta para dicha participación, el registro de los alumnos mediante una dirección de correo electrónico que resulta visible y accesible al resto de los alumnos que se encuentren registrados en los mismos, la mayoría de los cuales son menores de dieciocho años. Asimismo, según se expone en dicha consulta, en algunos supuestos se ha utilizado esta plataforma para remitir "correos insultantes" entre compañeros, por lo que han surgido dudas acerca de la adecuación de dichos cursos on-line a la normativa sobre protección de datos.
Conforme indica el artículo 2.1 de la LOPD, "La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". A estos efectos, debe recordarse que, según el artículo 3 b) de la Ley, se entiende por fichero "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".
Ello supone que la existencia de un sitio Web no implica necesariamente la inclusión del mismo en ningún registro de la Agencia de Protección de Datos de la Comunidad de Madrid, sin perjuicio de que cuando en el mismo se recopilen o publiquen datos de carácter personal y se constituya un fichero, sí resulte de aplicación la Ley Orgánica. En consecuencia los sitios Web no se encuentran inscritos en el Registro de ficheros de esta APDCM ni, en su caso, en el Registro General de la Agencia Española de Protección de Datos, siendo únicamente inscritos los ficheros de datos de carácter personal que contienen información relacionada con personas físicas identificadas o identificables.
Además, la LOPD tiene su ámbito territorial de aplicación definido también en el artículo 2, según el cual la misma se aplicará a todo tratamiento de datos de carácter personal:
"a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional Público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito."
Ello ya nos permite considerar que la LOPD resulta plenamente aplicable a los tratamientos de datos de carácter personal efectuados por una persona o entidad de nacionalidad española que, en el marco de su actividad, recoge y somete a tratamiento, datos de carácter personal obtenidos en España. En consecuencia, de acuerdo con dicho precepto, cualquier tratamiento de datos realizado en el marco de un establecimiento situado en España deberán someterse a lo dispuesto en la legislación española.
En este sentido, conviene señalar que, a los efectos de la LOPD, se entenderá por datos de carácter personal cualquier información concerniente a personas físicas identificadas o identificables (artículo 3.a) de la Ley). Con base en la definición anterior será suficiente con que los datos permitan hacer identificable a la persona concreta para que se trate de datos de carácter personal.
Hecha la anterior precisión, la recogida de datos de carácter personal que puede producirse a través de un registro de usuarios en cursos on-line, vía Internet, deberá adecuarse a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, y a sus normas de desarrollo.
A su vez, los ficheros constituidos con la dirección de correo electrónico se someterán a la propia LOPD, en función de la información que contengan acerca de su titular.
La dirección de correo electrónico se forma por un conjunto de signos o palabras libremente elegidos generalmente por su titular, con la única limitación de que dicha dirección no coincida con la correspondiente a otra persona. Esta combinación podrá tener significado en sí misma o carecer del mismo, pudiendo incluso, en principio, coincidir con el nombre de otra persona distinta de la del titular.
De lo antedicho se desprende que podemos referirnos a dos supuestos esenciales de dirección de correo electrónico, atendiendo al grado de identificación que la misma realiza con el titular de la cuenta de correo:
El primero de ellos se refiere a aquellos supuestos en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo esta información referirse tanto a su nombre y apellidos como a la empresa en que trabaja o su país de residencia (aparezcan o no estos en la denominación del dominio utilizado. En este supuesto, a nuestro juicio, no existe duda de que la dirección de correo electrónico identifica, incluso de forma directa al titular de la cuenta, por lo que en todo caso dicha dirección ha de ser considerada como dato de carácter personal. Ejemplos característicos de este supuesto serían aquellos en los que se hace constar como dirección de correo electrónico el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel con el propio del Estado en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios (pudiendo incluso delimitarse el centro de trabajo en que se realiza la prestación).
Un segundo supuesto sería aquel en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con la persona titular de la cuenta (por referirse, por ejemplo, el código de la cuenta de correo a una denominación abstracta o a una simple combinación alfanumérica sin significado alguno). En este caso, un primer examen de este dato podría hacernos concluir que no nos encontramos ante un dato de carácter personal. Sin embargo, incluso en este supuesto, la dirección de correo electrónico aparecerá necesariamente referenciada a un dominio concreto, de tal forma que podrá procederse a la identificación del titular

mediante la consulta del servidor en que se gestione dicho dominio, sin que ello pueda considerarse que lleve aparejado un esfuerzo desproporcionado por parte de quien procede a la identificación. Por todo ello se considera que también en este caso, y en aras de asegurar, en los términos establecidos por la Jurisprudencia de nuestro Tribunal Constitucional, la máxima garantía de los Derechos Fundamentales de las personas, entre los que se encuentra el derecho a la "privacidad", consagrado por el artículo 18.4 de la Constitución, será necesario que la dirección de correo electrónico se encuentre amparada por el régimen establecido en la LOPD.

Junto con estos dos supuestos, debe añadirse, evidentemente, que si en un fichero -junto con la dirección de correo electrónico- aparecieran otros datos que permitieran la identificación del sujeto (tales como su nombre y apellidos, su número de teléfono o su domicilio, conjunta o separadamente), la identificación sería absoluta e indudablemente nos encontraríamos ante datos de carácter personal.

A la vista de lo que se ha venido indicando, cabe concluir que el tratamiento de los datos relacionados con una dirección de correo electrónico que goce de la consideración de dato de carácter personal, habrá de someterse a lo establecido en la Ley Orgánica, incluida su notificación al Registro de Ficheros de esta Agencia de Protección de Datos de la Comunidad de Madrid o, en su caso, al Registro General de Protección de Datos de la AEPD.

Dicho lo anterior, entre las obligaciones de las entidades públicas o privadas responsables de las páginas Web en la que se producen los registros de usuarios, está la de obtener el consentimiento del interesado para el tratamiento o posible cesión de sus datos y la de informar sobre los derechos que les asisten (de rectificación, cancelación, acceso y oposición), así como sobre la identidad y dirección del responsable y sobre el uso que se va a dar a esos datos. Estas obligaciones suelen cumplirse mediante formularios y cláusulas a los que se accede a través de enlaces como pueden ser "aviso legal" o "política de protección" siendo necesario, que los afectados no puedan introducir dato alguno en la base de datos sin antes tener conciencia del citado aviso y "aceptarlo", haciendo un "click" en el lugar correspondiente.

Por otro lado, el consentimiento al que hacíamos referencia deberá ser, tal y como prevé el artículo 3 i) de la propia Ley Orgánica, libre, inequívoco, específico e informado, con indicación al afectado de la totalidad de los extremos a los que se extiende el deber de información, consagrado por el artículo 5.1 de la propia LOPD.

Ese consentimiento informado habrá de recabarse de tal forma que resulte imposible la introducción de dato alguno sin que previamente el afectado haya conocido la advertencia que contenga las menciones a las que nos hemos referido, pudiendo servir como prueba del consentimiento la acreditación de que el programa impide introducir los datos sin antes haber aceptado el aviso legal al que hemos hecho mención. Todo ello tiene por objeto asegurar que el consentimiento de los afectados sea efectivamente específico e inequívoco, tal y como exige la Ley Orgánica.

Para el supuesto de que la página Web o Portal de Internet a través del cual se realice el registro de datos personales corresponda a una entidad pública de la Comunidad de Madrid, para la recogida de dichos datos su responsable deberá incorporar una cláusula informativa del siguiente tenor:

""Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla), y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es (indicarla), de todo lo cual se informa en cumplimiento del art. 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal".

Tal y como se ha indicado, la citada cláusula podría figurar dentro de la política de privacidad de la página Web en cuestión.
A su vez, corresponde al Responsable de la página Web, y en todo caso al Responsable de la página Web www.educa.madrid.org la notificación al Registro de Ficheros correspondiente de la creación del fichero de datos creado a través de la página Web y el tratamiento informático posterior que va a realizar con los datos personales que se recojan, tal y como impone la LOPD.
En el supuesto concreto de la página Web www.educa.madrid.org, según consta en el Registro de ficheros de esta Agencia de Protección de Datos de la Comunidad de Madrid, aparece declarado e inscrito el correspondiente Fichero "EDUCAMADRID (USUARIOS REGISTRADOS DEL PORTAL EDUCATIVO DE LA CONSEJERIA DE EDUCACION)", figurando como responsable del mismo la Consejería de Educación de la Comunidad de Madrid, cuya finalidad declarada es "Autenticar a los usuarios del portal educativo con el fin de acceder a la Intranet y disponer de recursos y herramientas con finalidad educativa".
En consecuencia, según se aprecia, tratándose de un fichero público del ámbito de actuación de la Agencia de Protección de Datos de la Comunidad de Madrid, se ha procedido a la creación, declaración e inscripción del fichero, siguiendo para ello el procedimiento previsto en el artículo 4 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, y desarrollado posteriormente por el Decreto 99/2002, de 13 de junio, de regulación del procedimiento de elaboración de disposiciones de carácter general de creación, modificación y supresión de ficheros que contienen datos de carácter personal, así como su inscripción en el Registro, con carácter previo a su puesta en funcionamiento.
Tratándose de páginas Web creadas de titularidad privada, deberá proceder a la inscripción de sus ficheros en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos, conforme a lo establecido en la LOPD, siguiendo para ello el procedimiento previsto en el artículo 26 de dicha Ley Orgánica.
Tal y como se ha señalado, en ambos casos, el responsable del fichero deberá dar cumplimiento al derecho de información al interesado, con carácter previo a la recogida de sus datos, de acuerdo con lo previsto en el citado artículo 5 de la LOPD, así como recabar su consentimiento para el tratamiento de sus datos personales.
Por otra parte, por lo que se refiere a la publicación en el foro de la página Web correspondiente de "correos insultantes" sobre cualquiera de los usuarios registrados en el foro, dicha publicación podría resultar contraria tanto a lo dispuesto en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar, y a la propia imagen, como a lo previsto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
Así, conforme al artículo 18.1 de la Constitución, los derechos al honor, a la intimidad personal y familiar y a la propia imagen tienen el rango de fundamentales, y hasta tal punto aparecen realzados en el texto constitucional que el artículo 20.4 dispone que el respeto de tales derechos constituya un límite al ejercicio de las libertades de expresión que el propio precepto reconoce y protege con el mismo carácter de fundamentales.
De tal suerte, si un invitado o usuario registrado en un foro realiza dicho tipo de manifestaciones, a nuestro juicio, su acción no quedaría amparada por el artículo 20.1.a) de la Constitución Española, en virtud del cual, se reconoce y protege el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra o el escrito o cualquier otro medio de reproducción, toda vez que dicho precepto resulta aplicable siempre y cuando las opiniones se refieran a la gestión política-administrativa de los cargos públicos.
Tal y como se ha adelantado, del supuesto sometido al presente informe podría derivar responsabilidad por vulneración de lo dispuesto en la normativa sobre

protección de datos personales, tanto en relación con la persona que manifiesta dichos datos personales, como respecto del titular de la página Web en la que se procede a la publicación de los mismos.
En consecuencia, si algún usuario vertiese insultos, citando los datos de carácter personal de otros alumnos registrados en el curso on-line, no se deberían publicar dichos datos personales, ya que en caso contrario se vulneraría también el derecho a la protección de los datos personales de dichos alumnos.
En conclusión, la recogida de datos de carácter personal que puede producirse a través de un registro de usuarios en un Portal de Internet (con independencia de que un usuario se registre en uno o varios foros), deberá adecuarse a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, y a sus normas de desarrollo.
Lo dispuesto en la LOPD resulta de obligado cumplimiento, pudiendo su vulneración ser constitutiva de infracción leve, grave o muy grave. En los artículos 44, 45 y 46 de la propia Ley Orgánica quedan perfectamente descritos los tipos de infracciones que pueden dar lugar a la iniciación del correspondiente expediente sancionador, así como las especialidades relativas a la comisión de infracciones e imposición de sanciones en el ámbito de las Administraciones Públicas.
Finalmente, en cuanto a si los datos, tratándose de menores de edad, deben recabarse de los propios menores o de sus padres o tutores, será necesario analizar en qué supuestos se considerará que los mismos ostentan pleno discernimiento para prestar ese consentimiento y en cuáles aquél habrá de completarse con el de su representante legal.
A nuestro juicio, deben diferenciarse dos supuestos básicos, el primero referido a los mayores de 14 años, a los que la Ley atribuye capacidad para la realización de determinados negocios jurídicos, y el segundo, al consentimiento que pudieran prestar los menores de dicha edad.
Respecto de los mayores de catorce años, debe recordarse en primer término, que el artículo 162.1º del Código Civil exceptúa de la representación legal del titular de la patria potestad a "los actos referidos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".
Se plantea entonces si, en el supuesto de mayores de catorce años, ha de considerarse que el menor tiene condiciones suficientes de madurez para prestar su consentimiento al tratamiento de los datos, debiendo, a nuestro juicio, ser afirmativa la respuesta, toda vez que nuestro ordenamiento jurídico viene, en diversos casos, a reconocer a los mayores de catorce años la suficiente capacidad de discernimiento y madurez para adoptar por sí solos determinados actos de la vida civil. Baste a estos efectos recordar los supuestos de adquisición de la nacionalidad española por ejercicio del derecho de opción o por residencia, que se efectuará por el mayor de catorce años, asistido de su representante legal, o la capacidad para testar (con la única excepción del testamento ológrafo) prevista en el artículo 662.1 para los mayores de catorce años.
Por otra parte, debe recordarse que, según tiene señalado la Dirección General de Registros y del Notariado, en Resolución de 3 de marzo de 1989, "no existe una norma que, de modo expreso, declare su incapacidad para actuar válidamente en el orden civil, norma respecto de la cual habrían de considerarse como excepcionales todas las hipótesis en que se autorizase a aquél para obrar por sí; y no cabe derivar esa incapacidad ni del artículo 322 del Código Civil, en el que se establece el límite de edad a partir del cual se es capaz para todos los actos de la vida civil, ni tampoco de la representación legal que corresponde a los padres o tutores respecto de los hijos menores no emancipados". En resumen, la minoría de edad no supone una causa de incapacitación (de las reguladas en el artículo 200 del Código Civil), por lo que aquélla habrá de ser analizada en cada caso concreto a los efectos de calificar la suficiencia

en la prestación del consentimiento en atención a la trascendencia del acto de disposición y a la madurez del disponente.
Refrendando esta tesis, el artículo 13 del nuevo Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD, establece que:
"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.
3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.
4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales".
En consecuencia, a tenor de las normas referidas, cabe considerar que los mayores de catorce años disponen de las condiciones de madurez precisas para consentir, por sí mismos, el tratamiento automatizado de sus datos de carácter personal. Respecto de los restantes menores de edad, deberá estarse a lo dispuesto en el artículo 13 del Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD.
De acuerdo con lo anterior, la solución al supuesto planteado en la pregunta, esto es, la posibilidad de recabar directamente de un menor sus datos personales, sin contar con la autorización de sus padres o tutores legales, no depende del tipo de dato personal de que se trate, ni debe vincularse al diferente nivel de protección que la Ley confiere al dato personal en atención a la naturaleza de la información tratada y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. Por el contrario, la solución a cada caso concreto se extraerá de lo expuesto anteriormente en relación con los mayores de catorce años, o con los menores de dicha edad, de acuerdo con lo establecido en la normativa a que se ha hecho referencia.
Por tanto, a la vista de lo anteriormente señalado, con independencia del tipo de dato personal de que se trate, será necesario recabar el consentimiento de los menores para la recogida de sus datos, con expresa información de la totalidad de los extremos contenidos en el artículo 5.1 de la Ley Orgánica, recabándose, en el caso de menores de catorce años el consentimiento de sus representantes legales.

¿Puede imputarse a un Centro Escolar la vulneración de la privacidad de los datos personales de un alumno si un grupo de padres de los alumnos remite a otro padre, madre o tutor, un escrito -a su domicilio- recordándole la deuda que voluntariamente adquirió para material escolar, sin que el Colegio interviniera en tal acuerdo?

Con carácter general, no. Antes se tendría que demostrar que los datos personales del alumno y de sus padres han salido de algún fichero con datos personales de los que fuera responsable el centro docente y que el colegio hubiera intervenido en la utilización de éstos para reclamar el pago de la cuota en concepto de material.

¿Qué requisitos hay que cumplir para poder entregar datos personales a entidades bancarias y cajas de ahorros para gestionar pagos y cobros del Centro Educativo?

Para garantizar el cumplimiento de la legislación en materia de protección de datos personales, existen dos formas alternativas de plantear tal entrega:
- Como cesión de datos: en este caso, es imprescindible el consentimiento individual de cada uno de los afectados cuyos datos bancarios se entregan a la entidad financiera para que tramite el pago o cobro correspondiente.
- Como "tratamiento de datos" por la entidad financiera por cuenta del centro educativo. En este caso no es preciso el consentimiento individual de cada uno de los afectados, pero sí debe existir un contrato específico entre el centro educativo y la entidad financiera que contemple expresamente que el encargado del tratamiento (en este caso, la entidad financiera) únicamente tratará los datos personales conforme a las instrucciones del centro educativo, que no los utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas u organizaciones. En el contrato habrán de estipularse también las medidas de seguridad que aplicará la entidad financiera en relación con los datos personales que está tratando.

Medidas de seguridad

¿Todos los ficheros que contengan datos de carácter personal deben cumplir las mismas medidas de seguridad?

No. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información. Con carácter general, todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
Los centros públicos de educación tendrán que implantar las medidas de seguridad adecuadas al grado de protección que requieran los datos contenidos en cada uno de los ficheros, atendiendo a lo dispuesto en el Título VIII, "De las medidas de seguridad en el tratamiento de datos de carácter personal", del Real Decreto 1720/2007, de 21 de diciembre.
Si bien -con carácter general- todos los ficheros manejados por los centros de enseñanza que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico, en todos aquellos ficheros en los que se contengan datos de salud (por ejemplo, en los ficheros en los que se guarda información sobre absentismo del personal docente, o sobre enfermedades de los alumnos que deban tenerse en cuenta para la prestación del servicio del comedor, etcétera), deberán implantarse medidas de seguridad de nivel alto.

¿Quién debe ser el responsable de seguridad?

El Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, define al responsable de seguridad como la persona que, nombrada por el responsable del fichero, le ayuda a implantar, coordinar y controlar las medidas de seguridad. Debe tener la autoridad suficiente para implantar y vigilar el cumplimiento de las medidas de seguridad por parte del resto de los usuarios del fichero.

¿Es necesario presentar ante la Agencia de Protección de Datos el Documento de Seguridad de los ficheros automatizados de datos de carácter personal?

De conformidad con el Reglamento de desarrollo de la LOPD, los ficheros de datos personales deberán adoptar el nivel de seguridad básico, medio o alto, dependiendo del tipo de datos que manejen. Las medidas de seguridad que se adopten en virtud de los distintos niveles de seguridad existentes, han de estar recogidas en un Documento de Seguridad.
El Documento de Seguridad es de carácter interno, y si bien no es necesario presentarlo ante la Agencia de Protección de Datos, ha de estar disponible y actualizado por si ésta lo requiriera.

¿Se puede cifrar el nombre y apellidos de los posibles adjudicatarios de plazas de Educación de Adultos en los Centros Penitenciarios mediante el sistema de concurso de traslados?

Con carácter general, hay que señalar que en las provisiones de puestos de trabajo del personal funcionario rige el principio de publicidad, tal y como establece el artículo 20.1 c) de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, que expresamente prevé que las convocatorias para proveer puestos de trabajo por concurso o por libre designación, así como sus correspondientes resoluciones, deberán hacerse públicas en los Boletines o Diarios Oficiales respectivos por la autoridad competente para efectuar los nombramientos.
La LOPD regula en su artículo 6.4 LOPD un supuesto muy concreto referente al derecho de oposición, estableciendo que en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.
Teniendo en cuenta que en este caso la publicación de la adjudicación de los puestos de trabajo de Educación de Adultos en los Centros Penitenciarios puede conllevar un problema de seguridad física de los profesionales que obtengan destino en dichos puestos de trabajo al ser públicos sus datos personales, y sin perjuicio del principio general de publicidad de la convocatoria y de la resolución del concurso de traslado, podría resultar de aplicación el artículo 6.4 de la LOPD, permitiendo que los participantes en el concurso de traslados ejerciesen su derecho de oposición si justificasen debidamente que la publicación de su nombre puede llevar aparejado algún tipo de perjuicio para su seguridad física. En el caso de acceder a su petición, se podrían cifrar sus datos en la Resolución de adjudicación de puestos que se publique en el Boletín Oficial de la Comunidad de Madrid.
Sería conveniente que la Resolución de la Dirección General de Recursos Humanos de la Consejería de Educación por la que se convocara el concurso de traslados, contuviera una Base en la que se hiciese referencia a la posibilidad por parte de los participantes de ejercitar su derecho de oposición según lo dispuesto en el artículo 6.4 de la LOPD. Igualmente, en la solicitud para poder participar en el concurso de traslados sería adecuado que apareciese un apartado en el que el aspirante pudiera ejercitar tal derecho, mencionándose asimismo en las Instrucciones para cumplimentar la citada solicitud. De esta forma sería más fácil el ejercicio del derecho de oposición.
A modo de ejemplo, la Resolución podría incluir el siguiente texto: "De conformidad con lo establecido en el artículo 6.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, los maestros que resulten adjudicatarios de puestos de trabajo de Educación de Adultos en los Centros Penitenciarios, podrán ejercitar su derecho de oposición a la publicación de su nombramiento de tal forma que, en la Resolución de adjudicación de plazas que se publique en el Boletín Oficial de la Comunidad de Madrid, no aparezcan sus citados datos de carácter personal en relación con la plaza adjudicada en los Centros Penitenciarios, siempre que hayan justificado que esta publicación les puede deparar algún perjuicio a su seguridad física".

¿Qué medidas de seguridad deben aplicarse a un fichero de datos personales informatizado con datos especialmente protegidos ubicado en un único ordenador personal?

Deben aplicarse las medidas que se establecen para los ficheros de nivel alto en el RD 1720/2007, de 21 de diciembre. Entre estas medidas, deberá elaborar un documento de seguridad en el que se recojan las restantes medidas que deberán implantarse. Deberá asimismo designar un Responsable de Seguridad, que deberá controlar el tratamiento de datos que se realice y cumplir las obligaciones que le impone el RD 1720/2007 sin qué, en ningún caso, su designación suponga una delegación de la responsabilidad que corresponde al responsable del fichero.
El ordenador se deberá instalar en un lugar en el que se pueda establecer un control del acceso físico al mismo, no pudiendo estar en zonas comunes o espacios de libre acceso de personas.
Cualquier salida de información del sistema de tratamiento deberá realizarse cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte, además debe establecer un sistema de registro de las entradas y salidas de soportes.
Cuando el responsable del fichero sea el único usuario del mismo, y esta circunstancia quedase debidamente acreditada en el documento de seguridad, no será necesaria la implantación del registro de accesos. En el caso de que sean varios los usuarios y no se pueda garantizar la existencia de un sistema de registro de accesos, deberán aplicarse medidas alternativas, como el cifrado de los directorios donde se ubiquen los datos.
Si aún realizando el tratamiento de los datos en un local con acceso restringido, el ordenador personal en el que estén ubicados los datos se conectara a una red de telecomunicaciones, cada transmisión que se realizara por la misma requeriría el cifrado de los datos o la aplicación de cualquier otro mecanismo que garantizase que la información no sea inteligible ni manipulable por terceros. Esta medida no será obligatoria si la red de telecomunicaciones es una red privada.

¿Cómo debe interpretarse el control de acceso físico?

El control de acceso físico constituye una de las medidas de seguridad de nivel medio cuya implantación se exige por el Real Decreto 1720/2007, de 21 de diciembre, en cuyo artículo 99 se prevé que "Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información".
En relación con dicha cuestión, el consultante apunta dos posibles soluciones, indicando que "la redacción de dicho precepto podría estar haciendo referencia, exclusivamente a los locales donde estén ubicados los servidores (lo que es la sala de ordenadores propiamente dicha)"; y otra más amplia, que entiende que abarca cualquier local en el cual se encuentre ubicado un terminal a través del cual se pueda acceder a datos de carácter personal de ficheros de nivel medio o alto, incluido, por ejemplo, el local en que esté una impresora.
Por su parte, este nuevo Reglamento de desarrollo de la LOPD, en el artículo 2.m), define a los sistemas de información como "conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal".
La regulación establecida en dicho Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, para aplicar las medidas que garanticen un adecuado acceso a los ficheros que contengan datos de carácter personal, se circunscriben a las previsiones contenidas en los artículos 91 y 99 del mismo, en lo referente al establecimiento de controles de acceso y acceso físico para los ficheros sujetos a medidas de nivel básico y medio, y el artículo 103 relativo al registro de acceso a aquellos ficheros sujetos a medidas de nivel alto.

A su vez, el artículo 2.d) del Reglamento define el control de acceso como el "mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos". En estos términos, el artículo 91 se refiere al acceso como cualquier actuación por la que un usuario pueda tener conocimiento directo de "aquellos recursos que precisan para el desarrollo de sus funciones".
Los locales en que se encuentren ubicados los equipos que den soporte a los sistemas de información con datos de carácter personal se considerarán un espacio con acceso restringido y únicamente el personal autorizado en el documento de seguridad podrá tener acceso. Su delimitación física (una habitación cerrada, una sala de ordenadores, etc.), será la que el responsable de seguridad considere conveniente, siempre y cuando el lugar reúna las necesarias condiciones de seguridad y se realice un control automático o manual del acceso que permita identificar y autorizar el acceso únicamente a las personas definidas en el documento de seguridad.
La consulta plantea cómo debe establecerse el mecanismo de control de acceso físico a los locales donde se encuentren ubicados los equipos sistemas de información, al que se refiere el artículo 99 del Reglamento. En particular, en cuanto al lugar en que debe establecerse el control, deberá ser aquél en que se produzca el acceso material a los ficheros, pudiendo variar desde el propio ordenador central o Host, (en caso de que el fichero pueda ser accesible desde cualquier terminal), los servidores en los que residen los sistemas de información con datos de carácter personal de nivel medio ó alto, a un determinado ordenador personal (en caso de que el fichero sólo se encuentre ubicado en el mismo).
En el caso de los PCs conectados a un HOST o servidor no sería aplicable ese control, puesto que los datos normalmente residen en el servidor o en el Host, salvo que se almacenen en sus discos duros este tipo de datos.
En el caso de las impresoras, hay que prestar especial atención a aquellas en las que se impriman listados masivos con este tipo de datos, como es el caso de la emisión de nóminas y en éste caso serían aplicables los controles de acceso físico. En el caso de la impresión de informes de forma discreta e individual, es decir no masiva, no serían aplicables esos controles, y estas impresoras podrían estar compartidas con otros usuarios, aunque cada usuario debe ser responsable de retirar los documentos lo antes posible, conforme vayan saliendo.

IV - CONSULTAS FRECUENTES SOBRE LA PROTECCIÓN DE DATOS EN EL CASO DE LAS UNIVERSIDADES PÚBLICAS (APDM)

1.1 Declaración de ficheros y responsabilidad

¿Qué ficheros deben declarar las universidades públicas de la Comunidad de Madrid, y cómo se declaran?

¿Pueden crearse y utilizarse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición en la que se crean?

¿Quién es el responsable de los ficheros que se utilizan en las universidades?

1.2 Derechos de los ciudadanos y deber de información

¿Es posible denegar el ejercicio del derecho de acceso que la LOPD reconoce a los ciudadanos por la dificultad o el elevado coste que puede suponer su ejercicio?

¿Cómo se puede dar cumplimiento al deber de información al ciudadano que establece la LOPD, con carácter previo a la recogida de sus datos?

¿Qué información ha de incluirse en los impresos contenidos en los sobres de matricula y pantallas de recogida de datos para efectuarla por Internet?

1.3 Cesiones de datos

1.3.1 Datos de alumnos

¿Las calificaciones académicas de los alumnos de la Universidad pueden publicarse en los tablones o en Internet?

¿Cuáles son las fórmulas legales de publicación de los resultados de los siguientes procesos: Prueba de Acceso a estudios universitarios (Selectividad), Prueba de Acceso a la Universidad de los Mayores de 25 años y Proceso de Ingreso?

¿Puede un profesor acceder al expediente académico de un alumno?

¿Los padres y tutores de los alumnos tienen derecho a solicitar las calificaciones académicas a la Universidad?

¿Puede una Universidad facilitar datos personales de estudiantes a una entidad de ahorro para elaborar una "Tarjeta-Carné"?

¿Puede la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid acceder a los ficheros de datos de los alumnos matriculados en las Universidades de la Comunidad de Madrid?

¿En qué casos procede la cesión de datos personales a la policía?

¿Puede la Fundación de una Universidad utilizar el correo electrónico de antiguos alumnos para enviarles información sobre cursos de formación y master?

¿Puede una Universidad publicar indiscriminadamente la información personal contenida en el archivo personal de un personaje político español de la Transición cedido a dicha Universidad?

¿Es conforme a la LOPD la exigencia establecida en el apartado 2 del número 11 de la Orden de 8 de julio de 1988, en relación con la expedición de duplicados de títulos universitarios oficiales?

1.3.2 Datos del personal de la Universidad

¿Se puede publicar en Internet el directorio: nombres y datos profesionales de contacto, de todo el personal de una Universidad?

¿Qué datos se puede facilitar a los Delegados de Prevención del Comité de Seguridad y Salud de la Universidad con el objeto de que se puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores para valorar sus causas y proponer las medidas oportunas?

¿En los procesos electorales, pueden los candidatos utilizar el censo electoral para dirigir una carta a todos los integrantes del censo para dar a conocer su programa?

¿Es lícita la cesión del dato de la dirección de correo electrónico del personal docente investigador de una Universidad en favor de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid para realizar una encuesta sobre "necesidades formativas sentidas por el profesorado universitario"?

¿Que requisitos debe cumplir un estudio realizado por una Universidad referido al personal docente y de investigación?

¿Cómo afecta la LOPD al Proyecto de Orden de la Consejería de Educación por la que se regula el procedimiento de concesión anual del complemento autonómico por méritos individuales del personal docente e investigador de las Universidades Públicas de Madrid? ¿Cumple la normativa sobre protección de datos personales la publicación en Internet y mediante listados en soporte papel de los resultados de la evaluación de todos los profesores solicitantes del complemento retributivo autonómico por méritos individuales del personal docente e investigador de la Universidades Públicas de la Comunidad de Madrid?

1.3.3 Otras consultas

¿Los datos recogidos para una determinada finalidad pueden utilizarse para cualquier otra que se pueda plantear a posteriori?

¿Puede una Universidad ceder datos al Defensor Universitario?

¿Una Universidad tiene obligación de declarar las direcciones IP que distribuya?

¿Qué requisitos debe cumplir un contrato de prestación de servicios, por ejemplo, de Outsourcing, que una Universidad pretende contratar con una empresa?

¿Puede el Servicio de Biblioteca Universitaria acceder a los datos personales de los alumnos relativos a sus discapacidades o limitaciones para favorecer y mejorar los servicios prestados a dichos alumnos?

1.4 Seguridad de los datos

¿Todos los ficheros que contengan datos de carácter personal, ¿deben cumplir las mismas medidas de seguridad?

¿Quién debe ser el responsable de seguridad?

¿Qué medidas de seguridad deben aplicarse a un fichero de datos personales informatizado con datos especialmente protegidos ubicado en un único ordenador personal?

¿Como debe interpretarse el control de acceso físico?

Las Universidades Públicas de la Comunidad de Madrid pueden dirigirse a la Agencia de Protección de Datos de la Comunidad de Madrid (apdcm@madrid.org) para plantear preguntas relacionadas con la interpretación de la legislación vigente en materia de protección de datos personales.

A continuación se detallan algunas de las consultas más frecuentes realizadas por las distintas Universidades Públicas de la Comunidad de Madrid:

1.1 Declaración de ficheros y responsabilidad

¿Qué ficheros deben declarar las universidades públicas de la Comunidad de Madrid, y cómo se declaran?
Deben declararse todos aquellos ficheros que contengan datos de carácter personal, tanto si son informatizados como manuales estructurados o mixtos, siempre que estén identificadas o sean identificables las personas titulares de los datos.

¿Pueden crearse y utilizarse ficheros que contengan datos de carácter personal sin que se haya publicado la disposición en la que se crean?

No se puede llevar a cabo la creación y utilización de ficheros de datos de carácter personal por parte de las universidades públicas sin la oportuna publicación de la disposición de carácter general. En este sentido la LOPD tipifica como infracción grave proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente.
De igual manera, la LOPD tipifica como infracción leve, cuando no sea constitutivo de infracción grave no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.

¿Quién es el responsable de los ficheros que se utilizan en las universidades?

La LOPD define al responsable de los ficheros de datos personales como la persona física y jurídica que puede decidir sobre el contenido, la finalidad y uso de los datos.
En el caso de las universidades el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia, teniendo capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza, como el rectorado, la facultad o escuela, los vicerrectorados, la secretaría general, la gerencia general, los servicios jurídicos, los servicios médicos, etc.
En todo caso la responsabilidad sobre cada fichero dependerá de lo que se establezca en los Estatutos de la Universidad. Así, por ejemplo, la responsabilidad sobre el fichero destinado a la gestión académica, recae normalmente sobre el Vicerrectorado de Alumnos, la del fichero con los datos de los títulos académicos recae sobre la Secretaría General, mientras que el fichero que elabora la nómina correspondería a la Gerencia, etc.
El responsable de un fichero debe indicarse expresamente en el correspondiente anexo de la disposición en la que se crea el mismo.
En el caso de que un fichero que comparta entre varios órganos o responsables los datos, la Ley 8/2001 de la Comunidad de Madrid establece que la responsabilidad recaerá sobre el órgano que ostente la representación legal de las funciones a las que el fichero da apoyo.

1.2. Derechos de los ciudadanos y deber de información

¿Es posible denegar el ejercicio del derecho de acceso que la LOPD reconoce a los ciudadanos por la dificultad o el elevado coste que puede suponer su ejercicio?

No. La LOPD ya prevé (y ya lo preveía la LORTAD desde 1992), que los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
No obstante, la LOPD limita el ejercicio de ese derecho a los ciudadanos, pudiendo ser ejercitado únicamente a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

¿Cómo se puede dar cumplimiento al deber de información al ciudadano que establece la LOPD, con carácter previo a la recogida de sus datos?

El Tribunal Constitucional ha definido el derecho a la protección de datos como el derecho fundamental a la autodeterminación informativa, en virtud del cual, debe ser el interesado el que decida quién puede tener sus datos y para qué se usan. Para que este derecho sea efectivo es necesario que el ciudadano sea informado previamente, al objeto de que pueda ejercer sus derechos de acceso, rectificación, cancelación y oposición.
Para dar cumplimiento a este deber de información pueden utilizarse diferentes medios; el medio principal previsto por la LOPD es la inclusión de textos informativos en los impresos y cuestionarios que se utilicen. Una forma subsidiaria, que únicamente debe utilizarse en los supuestos en que resulte imposible la utilización de dichos impresos, formularios o cuestionarios, es la colocación de carteles informativos, accesibles a los ciudadanos, en los puntos en que se realice la recogida de los datos. En este último caso, deberá prestarse especial atención a que la información que figure en los carteles sea completa y detallada, y no genérica, y en particular contemplar todo lo especificado en el artículo 5 de la Ley Orgánica de Protección de Datos de Carácter Personal (ver siguiente pregunta).
Debe analizarse en cada supuesto concreto, la forma de recogida de los datos, la naturaleza del colectivo del que se están recogiendo y la forma más efectiva para que se dé cumplimiento al deber establecido en la Ley.

¿Qué información ha de incluirse en los impresos contenidos en los sobres de matricula y pantallas de recogida de datos para efectuarla por Internet?

Con carácter general, siempre que se soliciten datos de carácter personal la LOPD obliga en su artículo 5 a que se cumpla con el derecho de información, es decir, previamente se ha de informar:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Igualmente señala dicho artículo que cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior, no siendo necesaria la información a que se refieren las letras b), c) y d) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
La Agencia de Protección de Datos de la Comunidad de Madrid viene recomendando la utilización del siguiente texto-tipo para el cumplimiento de las obligaciones derivadas del citado artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal:
"Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla), y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es (indicarla), todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."
En el Registro de Ficheros de Datos Personales de la Agencia de Protección de Datos de la Comunidad de Madrid, parte de cuya información es accesible en línea a través de Internet en www.apdcm.es, figuran inscritos todos los ficheros declarados, entre los que se encuentran los ficheros para la realización de la matricula de cada universidad, de donde se podrán recoger todos los datos necesarios para personalizar el texto informativo del Artículo 5.

1.3 Cesiones de datos

1.3.1 Datos de alumnos

¿Las calificaciones académicas de los alumnos de la Universidad pueden publicarse en los tablones o en Internet?

Los expedientes académicos de los alumnos no constituyen un procedimiento de concurrencia competitiva que justifique la publicación de las calificaciones (no existe una disposición de carácter general de la Universidad que apruebe la convocatoria previa del número total de aprobados de cada curso académico. El número de aprobados y de suspensos lo determinará cada profesor, en función de los conocimientos adquiridos y de la realización de los exámenes o pruebas que haya superado o no cada alumno).
No hay que confundir la publicación de estas calificaciones con la posibilidad de publicar los listados de aspirantes con sus resultados de un proceso selectivo tales como las pruebas de acceso a la Universidad, los premios extraordinarios de carrera, contratación de personal, etc-. En estos casos será posible la publicación siempre y cuando la convocatoria determine expresamente el lugar de publicación (tablones de anuncios, páginas Web etc.) y ello porque en estos supuestos rige el principio de publicidad y así viene previsto específicamente en el artículo 59.5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
Con carácter general, las notas de calificación de cada asignatura tienen como destinatario al alumno, anotándose en su expediente académico. En consecuencia la difusión de dichas notas de calificación a través de los tablones de anuncios de la Universidad o a través de Internet, constituye una cesión de datos de carácter personal de los alumnos. Para que pueda realizarse una cesión de datos personales debe existir consentimiento de los interesados o bien, entre otras excepciones

establecidas por la LOPD, deberá existir una norma con rango de Ley que exima de dicho consentimiento.
La disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, establece en su apartado tercero que "No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación".
Por otra parte, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece en su artículo 4 (principio de calidad de los datos) que los datos personales sólo podrán ser sometidos a tratamiento (lo que incluiría su cesión a terceros a través de la publicación) "cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".
En consecuencia, considerando tanto la habilitación legal existente para la publicación de las calificaciones como los límites que conlleva la aplicación del principio de calidad de los datos, sería posible la publicación de las calificaciones en tablones de anuncios o a través de Internet, siempre que el acceso se limite únicamente a las personas interesadas (por ejemplo, profesores y alumnos, dependiendo de la ubicación física de los tablones y en el caso de Internet a través de una Intranet o comunidad virtual con restricción de acceso) y no el público en general. Sería manifiestamente contrario a la legislación de protección de datos, puesto que vulneraría el principio de calidad de datos, la publicación de tales calificaciones en Internet de modo abierto, es decir, permitiendo a cualquier persona el libre acceso a las mismas. Asimismo, resulta contraria a la LOPD la lectura pública de notas ante los medios de comunicación, o la utilización de otros mecanismos similares sin restricciones.

¿Cuáles son las fórmulas legales de publicación de los resultados de los siguientes procesos: Prueba de Acceso a estudios universitarios (Selectividad), Prueba de Acceso a la Universidad de los Mayores de 25 años y Proceso de Ingreso?

Las convocatorias de este tipo de procedimientos constituyen un claro ejemplo de procedimientos selectivos en régimen de concurrencia competitiva, sujetos al principio de publicidad, siéndoles de aplicación lo dispuesto en el artículo 59 de la Ley 30/1992. En dicho artículo se establecen las normas para notificar los actos administrativos, estableciendo en su apartado 5 que la publicación del acto sustituirá a la notificación en el caso de que se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.
Tanto las pruebas de acceso a la Universidad para mayores de 25 años, como el procedimiento para las pruebas de acceso a estudios universitarios, son procedimientos administrativos de concurrencia competitiva y están sujetos al principio de publicidad. Para cumplir con el derecho de información del artículo 5 de la LOPD, se recomienda incluir en los formularios de solicitud la siguiente cláusula:
"Los datos personales recogidos serán incorporados y tratados en el fichero (indicar nombre), cuya finalidad es (describirla), y podrán ser cedidos a (indicar), además de otras cesiones previstas en la Ley. El órgano responsable del fichero es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es (indicarla), todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."

¿Puede un profesor acceder al expediente académico de un alumno?

En la medida en que un profesor tiene una relación directa con cada uno de sus alumnos tendrá legitimidad para acceder a los expedientes académicos de cada uno de ellos, siempre que dicho acceso tenga una finalidad académica y por tanto compatible con las finalidades declaradas del fichero. Sin embargo, hay que señalar que el acceso de los profesores al Fichero Expedientes de Alumnos o Gestión Académica no debería ser indiscriminado, sino que cada profesor debería tener acceso solamente a los datos de sus alumnos de ese año académico, pues no estaría justificada la finalidad del acceso a los datos del resto de los alumnos.
En consecuencia, el responsable del fichero deberá establecer los controles de acceso necesarios para cumplir con esta medida, teniendo en consideración lo previsto en el artículo 91 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

¿Los padres y tutores de los alumnos tienen derecho a solicitar las calificaciones académicas a la Universidad?

Si los alumnos son menores de edad, los padres y tutores tienen derecho a solicitar a la Universidad las calificaciones académicas de sus hijos.
Por el contrario, en el caso de que los alumnos sean mayores de edad no se podrán ceder, ya que constituiría una comunicación de datos personales no amparada por las excepciones que contempla la ley.
En concreto, en relación a los menores de edad, se plantea si en la cesión de sus datos académicos a sus padres o tutores sin su consentimiento, debe prevalecer la voluntad de un alumno menor de edad que no quiera que se faciliten sus calificaciones académicas a sus padres o tutores sobre la pretensión de éstos de acceder a dicha información, no pudiendo en dicho caso la Universidad atender dicha solicitud de los padres o tutores.
En cuanto a la posibilidad de ceder los datos académicos de los menores a sus padres o tutores sin el consentimiento de dichos menores afectados, ante todo, deberá considerarse que la comunicación de los datos al padre, madre, tutor o representante legal, supone una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley como "Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado."
Respecto de las cesiones, el artículo 11.1 prevé taxativamente que "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado." Este consentimiento sólo se verá exceptuado en los supuestos contenidos en el artículo 11.2 de la Ley, entre los que se encuentra la posibilidad de que una norma con rango de Ley habilite la cesión.
En este supuesto, de acuerdo con lo dispuesto por el artículo 154 del vigente Código Civil, los hijos no emancipados están bajo la potestad del padre y de la madre. La patria potestad se ejercerá siempre en beneficio de los hijos, de acuerdo con su personalidad, y comprende los siguientes deberes y facultades:
1.- Velar por ellos, tenerlos en su compañía, alimentarlos, educarlos y procurarles una formación integral.
2.- Representarlos y administrar sus bienes (.....).
En consecuencia, dado que la facultad de acceder a la información de carácter académico (entre la que se cita la cesión relativa a las calificaciones obtenidas por los menores en la Universidad), se encuentra dentro del marco de los deberes y derechos que corresponden a los padres, inherentes al ejercicio de su patria potestad, cabe concluir que en el supuesto de los hijos no emancipados existe una norma legal

habilitante que ampara la cesión de los datos académicos de los menores a sus padres, derivada de lo previsto en el artículo 154 del Código Civil.
En lo que a los tutores se refiere, idéntica previsión, constitutiva de la habilitación legal exigida por el artículo 11.2 a) de la LOPD, se encuentra en lo dispuesto por el artículo 269 del citado Código Civil, cuando dispone que el tutor está obligado a velar por el tutelado y, en particular:
1. A procurarle alimentos.
2. A educar al menor y procurarle una formación integral.
3. A promover la adquisición o recuperación de la capacidad del tutelado y su mejor inserción en la sociedad.
4. A informar al Juez anualmente sobre la situación del menor o incapacitado y rendirle cuenta anual de su administración.
En consonancia con dicho precepto, para los tutores se obtienen similares consecuencias que las expuestas más arriba para los padres que ejercen la patria potestad, por lo que la cesión de los datos personales relativos a las calificaciones académicas de los menores resultará conforme con lo previsto por la Ley Orgánica de Protección de Datos de Carácter Personal.
En segundo lugar, se plantea si, dado que existe una relación jurídica entre la Universidad y los padres que no puede ser asumida por el menor, sería lícito facilitar dichas calificaciones como resultado de los servicios prestados. Además, se plantea si en el supuesto de que el alumno tuviera problemas de adaptación en la Universidad, el hecho de comunicarlo a sus padres podría ser constitutivo de infracción, conllevando la correspondiente sanción, de acuerdo con lo dispuesto en la LOPD. Igualmente, se plantea idéntica cuestión en el supuesto de que los datos sean solicitados por los servicios sociales de una Comunidad Autónoma que actúe como tutor del menor.
En relación con estas cuestiones, no resulta aplicable lo previsto por el artículo 11.2 c) de la Ley Orgánica 15/1999, cuando dispone que "el consentimiento exigido en el apartado anterior no será preciso (...) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros (…)", debiendo considerarse idéntica argumentación que la expuesta en los párrafos anteriores.
En consecuencia, con independencia de la existencia de una relación jurídica entre la Universidad y los padres o tutores del menor, la cesión de los datos relativos a las calificaciones académicas de éste, así como la comunicación de cualquier circunstancia relativa a la adaptación o inadaptación del menor en la Universidad, se encontrará amparada legalmente por los artículos 154 y 269 del vigente Código Civil.
Igualmente, en el supuesto de que los datos sean solicitados por los servicios sociales de la Comunidad de Madrid que actúe como tutor del menor, resultará aplicable la habilitación legal contenida en el artículo 269 del citado Código Civil, sin perjuicio de la existencia de otras normas de ámbito estatal y autonómico que ofrezcan idéntica cobertura en atención a las funciones legalmente conferidas a dicha Comunidad Autónoma cuando actúe en su condición de tutor del menor.

¿Puede una Universidad facilitar datos personales de estudiantes a una entidad de ahorro para elaborar una "Tarjeta-Carné"?

Con carácter general, los datos personales del estudiante únicamente podrán ser recogidos, tratados y cedidos, incluso sin el consentimiento del afectado, para el desarrollo y mantenimiento de la relación administrativa existente entre el alumno y la Universidad (vg. carné oficial de estudiante), y dentro del marco de las funciones administrativas atribuidas por la normativa aplicable a la propia Universidad.

Otro supuesto, diferente del anterior, es aquel en que la Universidad utiliza los servicios de un "Encargado del Tratamiento", que trata los datos personales por cuenta de la propia Universidad. En este caso, no se considerará comunicación de datos el acceso de la entidad que gestione la emisión del carné oficial cuando se limite a prestar dicho servicio a la Universidad, actuando por encargo de ésta y con estricto cumplimiento de lo previsto en el artículo 12 de la LOPD.
Para poder asociar los datos personales contenidos en el Carné oficial de estudiante a otras finalidades distintas de las anteriores, la Universidad deberá obtener el consentimiento del estudiante afectado. Así, por ejemplo, en el supuesto de que se pretenda la expedición de una "Tarjeta-Carné", vinculada a otro tipo de finalidades, tales como la financiera o crediticia, será necesario recabar el consentimiento del estudiante para la emisión de dicha Tarjeta cuya finalidad es distinta de la derivada de la relación administrativa existente entre alumno y Universidad, conforme a lo establecido en el artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
Sería contrario a lo previsto por la LOPD (artículo 4), por resultar claramente excesivo, que la Universidad impusiera al estudiante un tipo de Carné universitario que ineludiblemente se encontrara vinculado a una determinada tarjeta o a otro producto bancario. Para dicho supuesto, en todo caso, deberá contarse con el consentimiento del afectado, ofreciéndole otro tipo de Carné oficial alternativo, igualmente válido para el uso estrictamente académico.
En el supuesto de que el estudiante consintiera la emisión de la "Tarjeta-Carné", vinculada a otras finalidades distintas de las derivadas de la relación administrativa existente entre alumno y Universidad, también debería cumplirse con el principio de calidad de los datos respecto de qué datos son los que se han de facilitar a la Entidad financiera y con qué finalidad se usarán por dicha entidad. Los datos facilitados serán los exclusivamente necesarios para elaborar la "Tarjeta-Carné" y no se podrán usar con otras finalidades distintas de las consentidas por el estudiante. Además, terminada la relación de la persona en su condición de estudiante con la Universidad termina también la finalidad de la "Tarjeta-Carné", debiéndose proceder por la Entidad a cancelar dichos datos y a no usarlos para ofertar otros productos al sujeto afectado, ni durante su condición de estudiante ni, con más motivo, cuando deja de serlo.

¿Puede la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid acceder a los ficheros de datos de los alumnos matriculados en las Universidades de la Comunidad de Madrid?

Entre las actividades de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, recogidas en el artículo 5 de la Ley 15/2002, de 27 de diciembre, se encuentra la valoración de los servicios universitarios y de apoyo a los estudiantes y su posterior inserción laboral emitiendo posteriormente un informe sobre dicha situación.
Si dicha Agencia pretende realizar una encuesta a los alumnos de las Universidades Públicas de la Comunidad de Madrid para conocer su opinión sobre la calidad de los servicios y realizar un informe en el que se valoren los datos obtenidos, esta actividad va a conllevar el acceso a los datos personales de los estudiantes de las Universidades de Madrid.
En este caso, la cesión de datos necesaria para poder realizar la encuesta, sería una actividad que puede ser encuadrada en la excepción del consentimiento prevista en el artículo 11.2 e) de la LOPD. Por lo tanto, las Universidades de la Comunidad de Madrid podrían proceder a ceder los datos solicitados a la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid en la medida que dicha cesión tiene amparo legal.

Debe señalarse que todas las personas que intervengan en la realización de la encuesta, en la medida que están tratando datos de carácter personal, estarán sujetos por el deber de secreto de conformidad con lo previsto en el artículo 10 de la LOPD.

¿En qué casos procede la cesión de datos personales a la policía?

Los ficheros policiales poseen una regulación especial contenida en el artículo 22 de la LOPD y con base en ella, la recogida y tratamiento para fines policiales de datos de carácter personal de las universidades publicas, por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.
Este artículo habilita a las Fuerzas y Cuerpos de Seguridad del Estado para la obtención y tratamiento de los datos, lo que llevará aparejada la procedencia de la cesión instada, siempre y cuando se cumplan las siguientes condiciones:
o Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales. La obtención de los datos por parte de la Policía deberá basarse en dichas razones y, tratándose de datos especialmente protegidos, los datos deberán resultar absolutamente necesarios para los fines de una investigación concreta. En todo caso la cesión quedará limitada al uso derivado de la función de mantenimiento de la seguridad pública.
o Que se trate de una petición concreta y específica, al no ser compatible con lo señalado las solicitudes masivas de datos. La petición se limitará a datos personales concretos, debidamente individualizados, solicitados por las Fuerzas y Cuerpos de seguridad en el marco de las competencias que tengan atribuidas por la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.
o Que la petición se efectúe con la debida motivación, que acredite su relación con lo supuestos que se han expuesto, dejando constancia de la petición. La petición policial, debidamente motivada, se dirigirá al Responsable del tratamiento, acreditándose la existencia de una investigación policial en curso. La solicitud deberá cursarse a través de un soporte documental que permita dejar constancia de la misma, resultando admisible a dichos efectos la expedición de un oficio u orden de servicio extendidos por parte de la propia Policía encargada de las actuaciones.
o Que los datos sean cancelados cuando dejen de ser necesarios para las averiguaciones que motivaron su almacenamiento, en cumplimiento del artículo 22.4. Corresponderá a las Fuerzas y Cuerpos de Seguridad cesionarios garantizar la confidencialidad y seguridad de los datos personales cedidos.
La policía local, de acuerdo con la Ley Orgánica 2/1986, de 13 de marzo, Reguladora de las Fuerzas y Cuerpos de Seguridad del Estado, de las Policías de las Comunidades Autónomas y de las Policías Locales, y de la Ley 4/1992, de 8 de julio, de Coordinación de Policías Locales de la Comunidad de Madrid, puede ejercer funciones de policía judicial, así como efectuar diligencias de prevención y cuantas actuaciones tiendan a evitar la comisión de actos delictivos en el marco de colaboración establecido en las Juntas de Seguridad.
Se recoge por tanto una especialidad justificada al regular la recogida y tratamiento por parte de las Fuerzas y Cuerpos de Seguridad de datos de carácter personal para fines policiales, en los supuestos en que dicha recogida y tratamiento no cuente con el consentimiento de las personas afectadas. En esos casos, el responsable del fichero, habrá de responder a la solicitud de información que harán los miembros de la policía local, siempre que la petición se realice de forma concreta y específica, al no ser

compatible el ejercicio de solicitudes masivas de datos. La petición habrá de recoger igualmente la debida motivación y contemplar el cumplimiento del apartado 4 del mismo artículo 22 de la LOPD, según el cual los datos han de ser cancelados cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.
Por otra parte, la Disposición Adicional Quinta de la Ley Orgánica 4/2000, de 11 de enero, reguladora de los derechos y libertades de los extranjeros en España y su integración social, a partir de la reforma introducida por la Ley Orgánica 14/2003, de 20 de noviembre, en relación con el acceso a la información y colaboración entre Administraciones públicas, establece que:
"1. En el cumplimiento de los fines que tienen encomendadas, y con pleno respeto a la legalidad vigente, las Administraciones públicas, dentro de su ámbito competencial, colaborarán en la cesión de datos relativos a las personas que sean consideradas interesados en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo.
2. Para la exclusiva finalidad de cumplimentar las actuaciones que los órganos de la Administración General del Estado competentes en los procedimientos regulados en esta Ley Orgánica y sus normas de desarrollo tienen encomendadas, la Agencia Estatal de Administración Tributaria, la Tesorería General de la Seguridad Social y el Instituto Nacional de Estadística, este último en lo relativo al Padrón Municipal de Habitantes, facilitarán a aquellos el acceso directo a los ficheros en los que obren datos que hayan de constar en dichos expedientes, y sin que sea preciso el consentimiento de los interesados, de acuerdo con la legislación sobre protección de datos."

¿Puede la Fundación de una Universidad utilizar el correo electrónico de antiguos alumnos para enviarles información sobre cursos de formación y master?

Si la Fundación de la Universidad tiene una forma privada de personificación, resultaría que, desde la óptica de la protección de datos, el supuesto planteado derivaría de la existencia de una previa cesión de datos realizada por una Administración Pública (Universidad) a una persona jurídica privada (Fundación), no siéndole de aplicación ninguna de las excepciones al consentimiento previstas en el artículo 11.2 LOPD. En consecuencia, para poder realizar dicha cesión de datos debe requerirse el consentimiento previo de los alumnos afectados de conformidad con lo previsto en el artículo 11.1 LOPD antes de proceder a la cesión de la Universidad en favor de la Fundación.
No obstante lo anterior, la propia Universidad sí podría dirigirse directamente a los antiguos alumnos para mantenerles informados sobre los cursos de formación y master, pues este tipo de información constituye una finalidad compatible con la finalidad de gestión del fichero de expedientes de alumnos y de gestión académica.

¿Puede una Universidad publicar indiscriminadamente la información personal contenida en el archivo personal de un personaje político español de la Transición cedido a dicha Universidad?

Debe considerarse que la reproducción y difusión de las cartas de otras personas (terceros) que obran en el archivo del personaje político español de la Transición, constituye una cesión de datos de las reguladas en el artículo 11 de la LOPD, por lo que deberá analizarse si es conforme a lo que éste establece.
La Ley 4/1993, de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid establece, en su artículo 5, que forman parte del Patrimonio Documental madrileño los documentos de cualquier época producidos, conservados o reunidos por,

entre otros, la Universidades y demás centros públicos de enseñanza radicados en el territorio de la Comunidad de Madrid.
El Título IV de la citada Ley 4/1993, de 21 de abril, regula el acceso a los documentos y su servicio. En su artículo 38.4 se determina como criterio a la hora de acceder a la documentación que, cuando la información contenida en los documentos afecte a la seguridad, honor, intimidad, propia imagen o cualesquiera otros datos cuya reserva tutelan las leyes, no podrán ser consultados salvo que medie consentimiento expreso de los afectados o en los caso y condiciones señalados por la legislación reguladora en esta materia.
En idéntico sentido se manifiesta el artículo 57.1.c) de la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español, en virtud del cual, los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de 25 años de su muerte si su fecha es conocida o, en otro caso, de 50 años a partir de la fecha de los documentos.
Como ya se ha indicado, el citado artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, establece como criterio general para las cesiones de datos personales, el consentimiento del afectado. Dicho consentimiento es también exigido por el artículo 38.4 de la Ley de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid, y por el artículo 57.1.c) de la Ley 16/1985, de 25 de junio, reguladora del Patrimonio Histórico Español, ya que la reproducción y difusión de las cartas puede afectar a la intimidad de los autores de las mismas.
Además, hay que tener en cuenta que la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen considera como intromisión ilegítima la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo. No obstante, no considera intromisión ilegítima si hay consentimiento expreso del afectado.
En conclusión, y de acuerdo a la normativa citada, para realizar la reproducción y difusión de las cartas es necesario el consentimiento expreso y previo de sus autores.

¿Es conforme a la LOPD la exigencia establecida en el apartado 2 del número 11 de la Orden de 8 de julio de 1988, en relación con la expedición de duplicados de títulos universitarios oficiales?

De acuerdo con lo dispuesto en el citado precepto, en caso de extravío de un título, será requisito previo e indispensable, a los efectos de la expedición del correspondiente duplicado, la publicación, en el BOE, de un anuncio mediante el cual se haga constar el supuesto extravío con objeto de propiciar, en su caso, las oportunas reclamaciones, correspondiendo la iniciativa para la publicación de dichos anuncios a la Unidad de Títulos de la propia Universidad.
Tal y como se ha expuesto, el régimen de las cesiones de datos se contiene en el artículo 11 de la LOPD. En dicho artículo, se establecen -por vía de excepción- una serie de casos en que el consentimiento del interesado no es preciso para la cesión de sus datos, destacando entre ellos el supuesto en que la cesión se encuentre amparada por una norma con rango de Ley.
Por tanto, será necesario que exista una norma con rango de Ley estatal o autonómica que habilite la cesión inconsentida de los datos, o en su caso, contar con el consentimiento de los interesados. En todo caso, debe recordarse que el artículo 4.2 de la Ley Orgánica exige que los datos sean tratados únicamente para la finalidad que motivó su recogida, sin que quepa emplear dichos datos personales para una finalidad distinta.

En este supuesto, la cesión de datos realizada mediante publicación del anuncio relativo al "extravío de un título" en el Boletín Oficial del Estado se encuentra recogida en el apartado 2º del número 11 de la Orden de 8 de julio de 1988, para la aplicación de los Reales Decretos 185/1985, de 23 de enero, y 1496/1987, de 6 de noviembre, en materia de expedición de títulos universitarios oficiales (BOE de 13 de julio).
Habida cuenta del carácter meramente reglamentario del precepto transcrito, y en atención a la carencia de una norma con rango de ley formal que habilite la cesión inconsentida de los datos personales de los afectados en aras de la obtención del correspondiente duplicado de su título universitario, el referido precepto resulta contrario a lo previsto por la LOPD.
Por su parte, en materia de inscripción y registro de Universidades y títulos universitarios, las únicas previsiones contenidas en la Ley Orgánica 6/2001, de 21 diciembre, de Universidades, modificada en este punto por la Ley Orgánica 4/2007, de 12 de abril, son las establecidas en su artículo 34 ("Títulos universitarios"), de acuerdo con el cual:
"1. Las universidades impartirán enseñanzas conducentes a la obtención de títulos oficiales y con validez en todo el territorio nacional y podrán impartir enseñanzas conducentes a la obtención de otros títulos.
2. Los títulos universitarios de carácter oficial y con validez en todo el territorio nacional deberán inscribirse en el Registro de universidades, centros y títulos, previsto en la disposición adicional vigésima. Podrán inscribirse otros títulos a efectos informativos. El Gobierno regulará el procedimiento y las condiciones para su inscripción".
Por su parte, en su Disposición adicional vigésima, relativa al "Registro de universidades, centros y títulos", se establece que:
"En el Ministerio de Educación y Ciencia existirá el Registro de universidades, centros y títulos. Este registro tendrá carácter público y en él se inscribirán, además de las universidades y centros, los títulos oficiales con validez en todo el territorio nacional. Podrán inscribirse también otros títulos a efectos informativos que expidan las universidades. El Gobierno regulará su régimen, organización y funcionamiento".
El análisis de la normativa a la que se ha hecho mención, no altera en absoluto el régimen general de cesión de datos anteriormente aludido. Así, de una parte, en modo alguno puede considerarse que los registros universitarios constituyan fuentes accesibles al público, siendo éstas las exclusivamente enumeradas, de forma taxativa, en el artículo 3 j) de la Ley Orgánica 15/1999, de 13 de diciembre, esto es, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico dirección e indicación de su pertenencia al grupo, así como los Diarios y Boletines Oficiales y los medios de comunicación. Y, de otra parte, de acuerdo con la normativa transcrita, no se extrae la existencia de habilitación legal alguna contenida en una norma con rango de Ley formal que ampare la publicación en el Boletín Oficial del Estado de los datos de carácter personal referidos en el apartado 2 del número Undécimo de la Orden de 8 de julio de 1988.
Por ello, debe concluirse que la información a la que alude la pregunta, incluso cuando se limite al título obtenido por un determinado estudiante, únicamente podrá cederse cuando exista el consentimiento previo del interesado, prestado de acuerdo con lo dispuesto por el artículo 11.1 de la LOPD. Dicho consentimiento podría entenderse únicamente concurrente en los supuestos en que las correspondientes solicitudes de expedición de duplicados de títulos universitarios oficiales vayan acompañadas de una autorización del interesado en orden a la publicación de sus datos personales en el Boletín Oficial del Estado.
En conclusión, sin perjuicio de otras consideraciones legales, como las relativas a la supremacía normativa de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección

de Datos de Carácter Personal, y su carácter de "lex posterior", que podrían significar la derogación directa de la referida Orden de 8 de julio de 1988, y, en consecuencia, la inaplicación de la misma por incompatibilidad de su contenido con lo previsto en la normativa sobre protección de datos de carácter personal, resulta evidente que la aplicación de lo dispuesto en el apartado 2 del número Undécimo de la mencionada Orden del Ministerio de Educación y Ciencia es claramente contraria a lo previsto por la Ley Orgánica de Protección de Datos.

En razón de dicha circunstancia, así como en atención a la derogación del Real Decreto 1496/1987, de 6 de noviembre, del que la mencionada Orden trae causa, operada por distintos Reales Decretos publicados posteriormente, no debería procederse a la publicación en el Boletín Oficial del Estado del correspondiente anuncio, comprensivo de los datos de carácter personal de los afectados por los extravíos de sus títulos oficiales, al resultar dicha previsión claramente contraria a la normativa sobre protección de datos.

1.3.2 Datos del personal de la Universidad

¿Se puede publicar en Internet el directorio: nombres y datos profesionales de contacto, de todo el personal de una Universidad?

En la medida que la publicación de datos personales en páginas Web implicaría una cesión de datos indiscriminada, dicha cesión se regula por lo previsto en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En consecuencia y no existiendo habilitación legal que permita esta publicación, para hacerlo, sería necesario que cada afectado (personal docente, administrativo y laboral) diera su consentimiento, debiendo la Universidad asimismo permitir que en cualquier momento pudiese oponerse a la misma, procediendo al borrado y cancelación de sus datos del sitio Web de la Universidad en Internet.
Como regla general, debe considerarse la necesidad de que la publicación en Internet se realice con el consentimiento del afectado y con una finalidad académica.
A este supuesto no le resulta aplicable la excepción establecida por el artículo 2.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la LOPD, cuando establece que dicho reglamento no se aplica a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en administraciones, órganos u otras entidades jurídicas.
En este sentido, los datos contenidos en dicho fichero no se limitan a los propios de los representantes legales de la Universidad, ni a los de las personas físicas de contacto que prestan sus servicios en aquélla, sino que comprenden, además, entre otros datos personales, los identificativos del personal docente, administrativo y de servicios de la Universidad.
Igualmente, en este caso, habría que evitar que se pudiesen confeccionar listados del directorio por aquellos que accedan al mismo, dado que la finalidad de dicho directorio es informativa y a estos efectos debería incluirse una leyenda informativa advirtiendo de que los datos y direcciones de correo electrónico de la Universidad que son objeto de publicación en el directorio "sirven únicamente a finalidades exclusivamente académicas y administrativas, y su empleo para cualquier uso distinto de los señalados, y en particular para fines comerciales o envío de correos basura "spam", será contrario a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y será puesto en conocimiento de las autoridades competentes en materia de protección de datos".
Sí podría publicarse el directorio, sin necesidad de consentimiento por parte de los interesados, en la red interna o Intranet de la Universidad (con acceso limitado al resto de personal de la Universidad y a los alumnos), considerando que el acceso se efectuaría en el ámbito de la relación administrativa y que la previsible finalidad de esa comunicación sería la de facilitar este tipo de relaciones. En este caso, el tratamiento de datos realizado mediante la publicación podría estar exceptuado de la prestación del consentimiento por aplicación de la excepción del artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que señala que no será necesario el consentimiento cuando los datos se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento. En cualquier caso, la Universidad debería cumplir igualmente con el deber de información contenido en el artículo 5.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
Sin perjuicio de lo anterior, el tratamiento del dato relativo a la dirección de correo electrónico del Personal Docente Investigador por parte de los cesionarios deberá vincularse al principio de calidad de los datos que recoge el citado artículo 4 de la Ley

Orgánica 15/1999, limitándose la utilización de los mismos a aquéllas finalidades que directamente se desprenden de lo dispuesto por la normativa referida.

¿Qué datos se puede facilitar a los Delegados de Prevención del Comité de Seguridad y Salud de la Universidad con el objeto de que se puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores para valorar sus causas y proponer las medidas oportunas?

La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales establece como competencia del Comité de Seguridad y Salud conocer y analizar los daños producidos en la salud o en la integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas (artículo 39.2.c).

Por lo tanto, puede tener acceso, sin contar con el consentimiento del afectado al concurrir la excepción de que una norma con rango de ley prevea la cesión, a un listado en que se incluya nombre y apellidos de los trabajadores accidentados, fecha del accidente, fechas de alta y baja, tipo de lesión/región anatómica y forma en que se produjo o agente que causó dicho accidente, siempre y cuando dicho conocimiento tengan como finalidad conocer y analizar los daños producidos en la salud o integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas.

El comité de empresa de la Universidad ha solicitado un listado nominativo de todos los empleados. ¿Debe entregarse? ¿Cuáles son los datos que pueden entregarse a los representantes sindicales?

Los datos que se deben facilitar al Comité de Empresa se encuentran regulados en el artículo 64 del Estatuto de los Trabajadores, en su número 1, en el que se indica que el comité de empresa tiene, dentro de sus competencias, las de recibir información del empresario sobre ciertos aspectos. El Comité de Empresa ejerce unas funciones de vigilancia y protección, sin necesidad de acceder a información diferente de la que marque la Ley.

A la vista de las previsiones legales que habilitan las funciones y competencias de las Secciones Sindicales, Comités de Empresa y Juntas de Personal que han sido detalladas en el apartado anterior, se considera que, de acuerdo con la LOPD, dichas previsiones no especifican con carácter general que se tenga que proceder a la cesión de datos personales de los empleados públicos en los siguientes supuestos: para conocer el establecimiento de la jornada laboral y horario de trabajo, régimen de permisos, vacaciones y licencias; emitir informe sobre materias como traslado total o parcial de las instalaciones, planes de formación de personal o implantación o revisión de sistemas de organización y método de trabajo; conocer las estadísticas sobre el índice de absentismo y sus causas, los accidentes en acto de servicio y enfermedades profesionales y sus consecuencias, los índices de siniestralidad, los estudios periódicos o especiales del ambiente y las condiciones de trabajo, así como las correspondientes a recibir información trimestral sobre política de personal.

Por tanto, con carácter general, estas funciones quedarán plenamente cumplidas por parte de las Administraciones públicas, mediante la cesión a las Secciones Sindicales, los Comités de Empresa y Juntas de Personal, de la información debidamente disociada, según el procedimiento definido en el artículo 3 f) de la LOPD, que permita a aquéllos conocer las circunstancias relativas a la política de personal sin referenciar la información en un sujeto concreto.

No obstante lo anterior y en el supuesto en que un empleado público haya planteado una queja ante su Sección sindical, Comité o Junta correspondiente, relativa a sus condiciones de trabajo, será posible la cesión del dato específico de dicha persona.

No obstante lo expuesto en el apartado anterior, hay que tener en cuenta, que el legislador puede prever específicamente aquellos datos de carácter personal de los trabajadores que pueden ser cedidos a las Secciones Sindicales, Comités de Empresa

y Juntas de Personal, y de esa forma, la necesidad del consentimiento de los afectados quedaría excepcionada. Por otro lado, no hay que olvidar la función de la Jurisprudencia constitucional y ordinaria en la interpretación tanto del derecho a la libertad sindical como del derecho fundamental a la protección de datos personales.
Entre los supuestos legales que contemplan las cesiones de datos, se podrían señalar, entre otros, los siguientes:
1. Será posible la cesión de los datos que figuren en la copia básica de los contratos de trabajo -artículos 64 y 8.3 del Estatuto de los Trabajadores-, dado que específicamente figura como información concreta a facilitar a los representantes de los trabajadores, con la excepción del DNI, el domicilio del trabajador, estado civil y cualquier otro dato que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo afecte a la intimidad personal de los empleados.
2. Igualmente, será posible la cesión en el caso de obtener información de las sanciones impuestas por faltas muy graves a los trabajadores -artículo 64 E.T. y artículo 9 de la Ley 9/1987-.
3. Por otra parte, en el caso del personal funcionario y respecto del complemento de productividad, el artículo 23.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, tras definir en su apartado c) el citado complemento, indica, en el último párrafo de este apartado, que "en todo caso, las cantidades que perciba cada funcionario por este concepto serán de conocimiento público de los demás funcionarios del Departamento u Organismo interesado así como de los representantes sindicales".
4. Asimismo en el caso de vigilancia de la salud, los artículos 36.2 b) y 39.2 c) de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, habilitan a que los Delegados de Prevención que forman parte del Comité de Seguridad e Higiene puedan conocer y analizar los daños producidos en la salud o integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas. En consecuencia y con las limitaciones previstas en el artículo 22.4 del mismo texto legal podrán tener acceso, por ejemplo, al nombre y apellidos de los trabajadores, fecha del reconocimiento médico, fechas de alta y baja y conclusiones del reconocimiento médico.
5. Igualmente el artículo 11.2 de la LOLS prevé que el empresario proceda al descuento de la cuota sindical sobre los salarios de los trabajadores afiliados y su transferencia al sindicato correspondiente, siempre que exista conformidad del trabajador. Es decir, aquí se trata de un supuesto de cesión de datos habilitados por ley (transferencia de la cuota sindical), pero que necesita del consentimiento del trabajador afectado, dado que el trabajador, para cumplir con su obligación del pago de la cuota, puede optar por su abono directo al sindicato sin necesidad de que la empresa se lo descuente de la nómina.
6. Por último y a los efectos de informar a todos los empleados públicos pertenecientes a cada uno de los ámbitos de negociación, de conformidad con el artículo 64.12 del Estatuto de los Trabajadores y el artículo 9.10 de la Ley 9/1987, de 12 de junio, y siguiendo la doctrina del Tribunal Constitucional (ver por ejemplo STC 142/1993, STC 213/2002 y la más reciente STC 281/2005) se entiende que podrían tener acceso al nombre, apellidos y la dependencia administrativa donde prestan sus servicios cada uno de dichos empleados públicos, así como a la dirección de correo electrónico en el supuesto de que la Unidad administrativa se la haya asignado.
En este último supuesto referido a facilitar la dirección de correo electrónico de los empleados a los representantes sindicales, hay que resaltar la importancia del uso al que puede ser destinado por estos y que viene reconocido en la propia sentencia 281/2005 del Tribunal Constitucional. Así, se señala que el derecho a enviar información sindical tanto a los afiliados como a los no afiliados forma parte del derecho de libertad sindical (FJ4), si bien está sujeto a límites o restricciones, como

son las referidas a que sólo se justifica su uso para transmitir información de naturaleza sindical y laboral …. Y que la comunicación no puede perturbar la actividad normal de la empresa (FJ8). En este sentido, señala el TC que resultaría constitucionalmente lícito que la empresa predeterminase las condiciones de utilización para fines sindicales de las comunicaciones electrónicas siempre que no las excluyera en términos absolutos (FJ8).
Por último, hay que señalar que de conformidad con el derecho de oposición reconocido en el artículo 6.4 LOPD, los empleados públicos que no quieran recibir información sindical pueden oponerse a este tratamiento, y la representación sindical como responsable del envío tendrá la obligación de dejar de enviar información a todos aquellos que hayan ejercitado este derecho.

¿En los procesos electorales, pueden los candidatos utilizar el censo electoral para dirigir una carta a todos los integrantes del censo para dar a conocer su programa?

En principio, dicha posibilidad debería preverse en la normativa que regule los procesos electorales en cada Universidad. Por tanto el Estatuto o el Reglamento Orgánico de la propia Universidad debería establecer la regulación del censo electoral y prever los datos que debe contener y el uso que se puede hacer del mismo en el procedimiento electoral por parte de cada candidatura.
Sin embargo, en cualquier caso, en las Universidades deben destacarse las funciones de carácter público y administrativo, relativas al control del cumplimiento de las normas de régimen electoral en los procesos de elección de sus órganos de gobierno y representación, así como de los demás derechos y obligaciones derivados del cumplimiento de los respectivos estatutos, regidos por el principio democrático y representativo. En este sentido, la LOU exige que las Universidades regulen su estructura interna y funcionamiento a través de sus Estatutos, de acuerdo con principios democráticos y representativos.
En materia electoral, el Fichero de censo electoral que sirve de base al proceso electoral ha de reputarse como fichero público, rigiéndose por lo dispuesto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y encontrándose sometido a lo dispuesto en el artículo 41.1 de la LOPD. El tratamiento y publicación de los datos contenidos en el censo tendrá por exclusiva finalidad garantizar el ejercicio por los electores de su derecho de sufragio, no siendo posible su utilización ni cesión para ninguna finalidad distinta de aquélla. En este sentido, queda prohibida cualquier información particularizada sobre los datos personales contenidos en el Censo Electoral.
En conclusión, en materia electoral, en aquellos supuestos en que los Estatutos de una determinada Universidad no se pronuncien, deberá acudirse a las normas básicas del Estado y a la legislación de la Comunidad de Madrid en la materia. Puesto que ha de tratarse de normas que regulen el proceso electoral, serán las contenidas en la Ley 5/1985, Orgánica Reguladora del Régimen Electoral General. Así lo ha considerado el Tribunal Supremo en varias sentencias (entre otras, la STS de 4 de Enero de 1980 y la STS de 7 de mayo del 2001). En ellas se señala que resulta de aplicación el artículo 41.5 de la LOREG y podrá proporcionarse la copia del censo a las candidaturas al día siguiente de ser proclamadas.

¿Es lícita la cesión del dato de la dirección de correo electrónico del personal docente investigador de una Universidad en favor de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid para realizar una encuesta sobre "necesidades formativas sentidas por el profesorado universitario"?

La cesión del dato de la dirección de correo electrónico del personal docente investigador de una Universidad en favor de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, para realizar una encuesta sobre necesidades formativas sentidas por el profesorado universitario, constituye también una auténtica comunicación de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999, como toda revelación de datos realizada a una persona distinta del interesado, que deberá someterse a lo dispuesto en el artículo 11 de la propia LOPD.

De acuerdo con el artículo 11.2 de la Ley Orgánica de Protección de Datos, será necesario que exista una norma con rango de Ley estatal o autonómica que habilite la cesión inconsentida de los datos, o en su caso, contar con el consentimiento de los interesados. De este modo, salvo que exista el consentimiento de los interesados, la cesión será admisible cuando exista una norma con rango de Ley, estatal o autonómica que habilite de forma expresa dicha comunicación a favor de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid.

El Titulo VII de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, se encuentra dedicado a la investigación en la Universidad, considerándola como una función esencial de la Universidades y asumiendo como uno de sus objetivos el desarrollo de la investigación científica. El artículo 31 de dicha Ley Orgánica se refieren a la "Garantía de Calidad de las Universidades", disponiendo que la promoción y la garantía de la calidad de las Universidades españolas, en el ámbito nacional e internacional, es un fin esencial de la política universitaria y tiene como objetivos, entre otros, la transparencia, la comparación, la cooperación y la competitividad de las Universidades en el ámbito nacional e internacional, la mejora de la actividad docente e investigadora y de la gestión de las Universidades, y la información a las Administraciones públicas para la toma de decisiones en el ámbito de sus competencias.

Dichos objetivos se cumplirán mediante la evaluación, certificación y acreditación de las actividades docentes, investigadoras y de gestión del profesorado universitario, las actividades, programas, servicios y gestión de los centros e instituciones de educación superior, y otras actividades y programas que puedan realizarse como consecuencia del fomento de la calidad de la docencia y de la investigación por parte de las Administraciones públicas. Las funciones de evaluación, y las conducentes a la certificación y acreditación, corresponden a la Agencia Nacional de Evaluación de la Calidad y Acreditación y a los órganos de evaluación que las leyes de las Comunidades Autónomas determinen, en el ámbito de sus respectivas competencias, sin perjuicio de las que desarrollen otras agencias de evaluación del Estado o de las Comunidades Autónomas.

En consecuencia, la realización por parte de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, de una determinada encuesta sobre necesidades formativas sentidas por el profesorado universitario, resultará relevante en relación con las funciones atribuidas a este tipo de Agencias de Calidad y/o Evaluación por la propia Ley Orgánica 6/2001, de 21 de diciembre, en función de los objetivos legalmente asumidos por estos entes de derecho público, relacionados con la evaluación de la calidad de los servicios prestados por las Universidades a la sociedad.

A su vez, en relación con el ámbito estatal, el artículo 32 de la Ley Orgánica de Universidades, autoriza la constitución de la denominada "Agencia Nacional de Evaluación de la Calidad y Acreditación", a la que se atribuyen el conjunto de competencias referidas en el transcrito artículo 31 de la propia Ley Orgánica 6/2001, de 21 de diciembre.

En conclusión, de los citados preceptos, contenidos en la normativa estatal sobre Universidades, se extrae la existencia de una habilitación legal expresa a favor de las Agencias de Evaluación, Calidad y Acreditación, tanto estatales como autonómicas, que ampararía la cesión de los datos de carácter personal correspondientes a las direcciones de correo electrónico del Personal Docente Investigador.
Idéntico razonamiento y cobertura legal pueden utilizarse en relación con la realización de encuestas sobre las necesidades formativas del personal docente investigador acometidas por parte de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, en razón de la existencia de una norma autonómica con rango de ley formal de la que se obtiene, igualmente, la habilitación legal suficiente para la comunicación de datos.
En este sentido, el artículo 1 de la Ley 15/2002, de 27 de diciembre, de la Comunidad de Madrid, de creación de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, crea -adscrita a la Consejería de Educación- la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, como ente de derecho público con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus fines. Como principios de la organización de dicha Agencia, se establecen la independencia de los órganos que participan en la evaluación, la objetividad y publicidad de los métodos y procedimientos empleados, la imparcialidad de los órganos de gestión y la participación de las Universidades en los programas de mejora de la calidad.
En virtud de lo dispuesto por su artículo 3.2 de dicha Ley autonómica, para el cumplimiento de sus fines, la Agencia podrá: b) Acceder a la documentación y archivos de las entidades objeto de evaluación y obtener la información que les solicite, de acuerdo con los procedimientos que se establezcan en los Estatutos y d) Realizar cualesquiera otras actividades que conduzcan al cumplimiento de sus fines.
Entre las Funciones de la Agencia de Calidad, a las que se refiere el artículo 4 de la Ley 15/2002, de 27 de diciembre, de la Comunidad de Madrid, se encuentran: a) La evaluación del Sistema Universitario de Madrid, a través del análisis del rendimiento de los servicios que presta y proponer las oportunas medidas de mejora de la calidad, c) La evaluación y acreditación de actividades docentes, investigadoras y de gestión del personal universitario, y e) La evaluación y acreditación de los programas, servicios y actividades de gestión de los centros e instituciones de educación superior.
Entre otras actividades desarrolladas por la Agencia para la consecución de sus fines, legalmente atribuidos, el artículo 5.1 de la tan citada Ley 15/2002, se refiere a las "Evaluaciones institucionales y para la acreditación de programas", y al "Análisis de las demandas socioeconómicas y la respuesta universitaria que reciben". Además, de acuerdo con el artículo 5.2 de dicha norma, "La Agencia podrá extender la oferta de sus servicios al análisis y evaluación de las necesidades o demandas de formación o de Investigación, Desarrollo e Innovación de los sectores empresariales o de producción, con cargo a la entidad pública o privada que solicite sus servicios, siempre que los análisis y evaluaciones solicitadas sean de interés para las funciones docentes e investigadoras de la Universidad."
Además, entre las funciones que el artículo 15 de la Ley encomienda al Comité de Dirección de la Agencia de Calidad, se encuentra la de proponer al Consejo Rector los planes anuales o plurianuales que se desarrollen de evaluación institucional y de acreditación de programas, de evaluaciones individuales de profesores, sobre valoraciones de la oferta de los estudios universitarios vigentes, de atención a los estudiantes y de inserción laboral, los que desarrollen análisis de las demandas socio-económicas y la respuesta universitaria que reciben, la evaluación de las necesidades de creación de Centros y los que se desarrollen en el ámbito de la cooperación internacional.

En conclusión, debe considerarse conforme con lo previsto por la LOPD la cesión del dato de la dirección de correo electrónico del personal docente investigador de una Universidad en favor de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid para realizar una encuesta sobre necesidades formativas sentidas por el profesorado, al aparecer vinculada a las funciones atribuidas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades y en la Ley 15/2002, de 27 de diciembre, de creación de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, referidas, entre otras, a la evaluación de la calidad de los servicios prestados por las Universidades a la sociedad y al análisis y evaluación de las necesidades o demandas de formación o de Investigación; la cesión se encuentra, por tanto, amparada en una habilitación legal.

¿Que requisitos debe cumplir un estudio realizado por una Universidad referido al personal docente y de investigación?

En el caso de que maneje datos personales, debe crear y registrar previamente el fichero donde tratar los datos, informar a los afectados y obtener su consentimiento previo, así como cumplir con las medidas de seguridad y demás requisitos previstos en la LOPD.

En el supuesto de que no se recabe dato personal alguno, no habría tratamiento de datos personales, por lo que el estudio quedaría fuera del ámbito de aplicación de la LOPD. Así, no existiría tratamiento de datos personales cuando los mismos se sometieran a un procedimiento previo de disociación, de modo que la información que se obtuviera no pudiera asociarse a personas identificadas o identificables.

A su vez, en el artículo 4.5 de la LOPD se contempla la posibilidad de que la finalidad científica o de investigación resulte compatible con la propia del fichero inicialmente creado, dando lugar -en su caso- al mantenimiento íntegro de determinados datos de acuerdo con la legislación específicamente aplicable.

¿Cómo afecta la LOPD al Proyecto de Orden de la Consejería de Educación por la que se regula el procedimiento de concesión anual del complemento autonómico por méritos individuales del personal docente e investigador de las Universidades Públicas de Madrid? ¿Cumple la normativa sobre protección de datos personales la publicación en Internet y mediante listados en soporte papel de los resultados de la evaluación de todos los profesores solicitantes del complemento retributivo autonómico por méritos individuales del personal docente e investigador de la Universidades Públicas de la Comunidad de Madrid?

De los Proyectos de Orden sometidos a informe de la Agencia de Protección de Datos de la Comunidad de Madrid en los últimos años, se desprende que los listados provisionales y definitivos relacionados con el procedimiento de concesión del complemento autonómico por méritos individuales del personal docente e investigador de las Universidades Públicas de la Comunidad de Madrid se van a publicar en la página Web de la Dirección General de Universidades e Investigación de la Consejería de Educación.

En este sentido, el artículo 11.1 de la LOPD establece que los datos de carácter personal, objeto de tratamiento, sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y cesionario con el previo consentimiento del interesado. Sin embargo, el apartado 2 del mismo artículo regula una serie de excepciones, entre las que se encuentra, referida al presente expediente, la posibilidad de que una norma con rango de ley establezca y regule las situaciones concretas en que la cesión de datos podrá tener lugar sin la necesidad del consentimiento de los afectados.

En este caso, la excepción legal que permite la publicación de los datos personales se contiene en el apartado 4 de la Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades que dice lo siguiente:
"4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación".
En concreto, dicho precepto permite la publicación de los resultados del procedimiento de concesión del complemento autonómico por méritos individuales del personal docente e investigador de la Universidades Públicas de la Comunidad de Madrid en la correspondiente página Web, siendo que dicho complemento se enmarca en un procedimiento de evaluación de la actividad docente e investigadora del personal al servicio de las Universidades Públicas de Madrid.
Ello no obstante, la habilitación legal contenida en este artículo se establece en favor de "las universidades y agencias o instituciones públicas de evaluación académica y científica".
En relación con la publicación de los listados provisionales, debe tenerse presente que, de conformidad con lo establecido en los artículos 59.6.b) y 60.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (RJPAC), dicha publicación se realiza a efectos de notificación, encuadrándose en el marco de un procedimiento en régimen de concurrencia competitiva.
A este tipo de procedimientos administrativos de concurrencia competitiva debe aplicárseles lo dispuesto en el referido artículo 59 de la Ley 30/1992, de 26 de noviembre. En dicho artículo se establecen las normas para notificar los actos administrativos, disponiendo su apartado 5 que la publicación del acto sustituirá a la notificación en el caso de que se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo.
Ello no obstante, de lo previsto en el apartado 4 de la Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, no se extrae que a la publicación (en forma de listados provisionales) de los datos personales correspondientes al expediente administrativo de los afectados por los tratamientos, y compresivos de una amplia variedad de datos de carácter personal, les resulte de aplicación la habilitación legal a la que se refiere dicho precepto, no pudiendo el Órgano consultante proceder a la publicación "en abierto" de dichos datos personales a través de Internet.
En este sentido, debe volver a señalarse la remisión expresa que la Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, realiza a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, cuando dispone en su apartado 1 que:
"1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.
Las Universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.
En conclusión, la publicación de los listados provisionales debería llevarse a cabo mediante su exposición en los correspondientes tablones de anuncios de los Órganos competentes o utilizando para ello los servicios propios de una Intranet administrativa (accesible únicamente a las personas interesadas en el procedimiento administrativo),

resultando excesiva su publicación -en abierto- a través de la página Web de la Dirección General de Universidades e Investigación, al resultar contraria dicha forma de publicación con lo dispuesto en la LOPD.
Por otra parte, sólo en razón de dicha notificación y de las posibles acciones derivadas de la misma, se explica la publicación de los listados provisionales, a través de los medios a los que se ha hecho mención, como parte integrante de los actos administrativos que componen dicho procedimiento. En consecuencia, dicha publicación (en los correspondientes tablones de anuncios o a través de una Intranet administrativa de acceso restringido) deberá ceñirse al plazo necesario e imprescindible para el ejercicio de las referidas acciones, realizándose a través de los medios apuntados, que se reputan como medios idóneos, y resultando de este modo conforme tanto al principio de transparencia administrativa como al derecho a la protección de datos de carácter personal.
De esta forma, cuando finalice el plazo de impugnación de diez días del "listado provisional" al que se refieren estas Órdenes, los datos de carácter personal publicados deberán ser retirados de los correspondientes "tablones de anuncios" de los Órganos competentes y/o -en su caso- deberán ser borrados de la Intranet administrativa utilizada que sirva de cauce para la notificación a los interesados, procediéndose a la cancelación de los mismos, puesto que según prevé el artículo 4.5 de la LOPD, los datos de carácter personal deben ser cancelados cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados, finalidad que en este caso no es otra, según se reitera, que la publicación a efectos de notificación.
En resumen, transcurrido el plazo fijado de diez días establecido para que los afectados puedan conocer su puntuación y también la del resto de los interesados, haciendo uso -en su caso- de dicho plazo para realizar las correspondientes reclamaciones, deberá procederse a la cancelación de los datos, mediante el bloqueo de dichos datos, procediendo a la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para las finalidades previstas por la legislación aplicable. En consecuencia, según se observa, sin perjuicio de lo previsto en relación con el tratamiento de los datos por el artículo 6.2 de la LOPD, a cuya aplicación apuntan estas Órdenes, debería preverse la cancelación de los datos personales una vez finalizado el plazo al que se ha hecho mención.
En síntesis, la publicación de los listados provisionales debería llevarse a cabo mediante su exposición en los correspondientes tablones de anuncios de los Órganos competentes o utilizando para ello los servicios propios de una Intranet administrativa con acceso restringido -mediante utilización de clave personal- a los interesados en el procedimiento, resultando excesiva su publicación -en abierto- a través de la página Web de la Dirección General de Universidades e Investigación, al resultar contraria dicha forma de publicación con lo dispuesto en la normativa sobre protección de datos de carácter personal, debiendo garantizarse -en todo caso- a través de estas Órdenes la cancelación de los datos personales cuando (artículo 4.5 LOPD) "hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados".
Por lo que respecta a los "Listados definitivos", de lo dispuesto en el apartado 4 de la Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, se extrae que a la publicación del "resultado del proceso de evaluación", esto es, a la publicación de la puntuación globalmente obtenida por cada uno de los afectados por el tratamiento, resulta de aplicación la habilitación legal a la que se refiere dicho precepto, incluso pudiendo el Órgano competente proceder a la publicación de dicho resultado definitivo "en abierto" a través de Internet, según se contempla en las Órdenes.

Sin embargo, de igual modo que en el supuesto anterior, una vez cumplida la finalidad de notificación debería proceder asimismo a la cancelación de los datos definitivos publicados en la página Web de la Dirección General de Universidades e Investigación (o de otro Órgano administrativo competente) y en los tablones de anuncios de las distintas Universidades, lo que, igualmente, debería preverse en estas Órdenes.
Además, el consentimiento del interesado en relación con la aplicación de lo dispuesto por el artículo 6.2 de la LOPD, no convalida un tratamiento de datos personales excesivos -más allá de la finalidad- que vulnere el principio de calidad ni una publicación de datos personales del expediente administrativo, no solo del resultado final. En este último caso, para que pueda publicarse información personal que exceda del resultado final del procedimiento no basta con el consentimiento inicial. Este consentimiento se refiere sólo al tratamiento de datos personales con la finalidad de obtener un complemento retributivo y no sirve para legitimar una publicación excesiva. Es necesario pedir un nuevo consentimiento para la publicación del resto de los datos personales, pudiendo el interesado no prestarlo. No es legítimo y no sería un consentimiento libre considerar que el que solicita el complemento retributivo tiene que admitir -so pena de renunciar a éste- una publicación excesiva y eterna de sus datos en Internet. Este consentimiento no sería un consentimiento libre sino viciado.
Tal y como se ha adelantado, lo anterior queda expresamente refrendado por el apartado 4 de la citada Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, toda vez que la misma se limita a establecer que: "Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación".
Hay que señalar que la publicación legítima en Internet de los listados de datos de profesores con el resultado final (puntuación definitiva) del procedimiento de concurrencia competitiva permite el acceso de cualquier persona pero esto no equivale a que estos listados sean fuentes accesibles al público a los efectos de posteriores tratamientos. Estas fuentes son las tasadas en la LOPD -el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación; art. 3.j) LOPD-. La utilización de esta información personal almacenada en sitios Web para finalidades distintas o su difusión en servidores distintos a los previstos en la propia convocatoria significaría una vulneración del principio de calidad de los datos -art. 4 LOPD- y del principio de consentimiento, que debe respetarse en cualquier tratamiento de datos personales -art. 6 LOPD-. Ahora bien, si el resultado final se publicase en el Boletín Oficial del Estado, de las Comunidades Autónomas o Provinciales, esta información con los datos de las personas que en ellos figuren sí se convertiría en una fuente de acceso público.
Finalmente, no obstante la habilitación legal conferida por el apartado 4 de la Disposición Adicional Vigésimo Primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, la Agencia de Protección de Datos de la Comunidad de Madrid recomienda como "mejor práctica" a la Dirección General de Universidades e Investigación que, en las próximas convocatorias del complemento autonómico por méritos individuales del personal docente e investigador de la Universidades Públicas de la Comunidad de Madrid, los listados definitivos correspondientes se publiquen a través de la Intranet de las Universidades y/o de la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid, de manera que sólo puedan acceder a dichos listados los miembros de la Comunidad Universitaria que hayan participado en la citada convocatoria o aquéllas personas que posean algún derecho o interés legítimo en

relación con la misma, puesto que de conformidad con el principio de calidad de datos del artículo 4.1 de la LOPD, los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para que se hayan obtenido.
A su vez, también en relación con el denominado "principio de calidad" de datos, recogido en el artículo 4 de la LOPD, según se ha adelantado, en la publicación de los "listados definitivos", las sucesivas Órdenes establecen la publicación de datos personales que resultan "excesivos", al prever que se publicará la puntuación total obtenida por cada profesor e investigador solicitante, así como cada uno de los criterios.
En este sentido, en atención a lo previsto respecto a las comunicaciones o cesiones de datos por el artículo 11 de la LOPD y de conformidad con el artículo 4.1 de la propia Ley Orgánica, se reitera que únicamente debería procederse a la publicación de la puntuación total obtenida por cada solicitante. Esto es, incluir la publicación de la puntuación relativa a sexenios reconocidos, proyectos de investigación y quinquenios representaría la revelación de datos excesivos y, por tanto, podría suponer una vulneración de la legislación sobre protección de datos de carácter personal.
Asimismo, los datos que se solicitan en los ANEXOS de estas Órdenes, relativos a "Número de proyectos fin de carrera dirigidos y aprobados" y "Número de tesis doctorales dirigidas y que hayan sido leídas y aprobadas, para el caso de que sea doctor y año de la última tesis aprobada" se estiman también excesivos, puesto que de dichas Órdenes no se desprende la necesidad de su solicitud, dado que no parecen tener ninguna relación con los criterios de valoración que figuran en la misma. En consecuencia, se propone que dichos datos personales no sean objeto de solicitud.

1.3.3 Otras consultas

¿Los datos recogidos para una determinada finalidad pueden utilizarse para cualquier otra que se pueda plantear a posteriori?

Los datos sólo se pueden recabar para cumplir una finalidad determinada, explícita y legítima, que además deberá conocer el interesado, como regla general, con carácter previo a la recogida de sus datos.
Los datos no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos, aunque la recomendación normal es que estas tareas se realicen con datos disociados, eliminando cualquier dato que identifique o permita identificar a las personas.

¿Puede una Universidad ceder datos al Defensor Universitario?

La Ley Orgánica 6/2001, de 21 de diciembre, prevé que el Defensor Universitario velará por el respeto a los derechos y las libertades de los profesores, estudiantes y personal de administración y servicios; en la medida que los datos a ceder por la Universidad al Defensor Universitario tengan como finalidad cumplir con la función descrita se podrá excepcionar el consentimiento expreso del afectado. En otro caso, el consentimiento será imprescindible.

¿Una Universidad tiene obligación de declarar las direcciones IP que distribuya?

Las autoridades de protección de datos están de acuerdo en que la dirección IP debe considerarse un dato de carácter personal.

Ha de destacarse el creciente uso de las llamadas direcciones estáticas, es decir, aquellas que se asignan permanentemente a una persona cuando contrata el servicio de acceso a Internet (en general, son las que se utilizan cuando se contratan servicios de banda ancha como ADSL o Internet por cable) frente a las direcciones dinámicas, que son asignadas en virtud de las que tiene disponibles un determinado proveedor de acceso a Internet en el momento de conexión del usuario, y cuya asociación con un usuario por parte de terceros tiene un grado mayor de dificultad.
Para los Proveedores de Acceso a Internet (PAI), es decir, aquellas entidades que proporcionan los medios técnicos necesarios para la conexión a la Red, la identidad del abonado asociado a una dirección IP es siempre conocida, independientemente de que se trate de una dirección estática o dinámica. En el caso de que el abonado sea una persona física el PAI conocerá su identidad y todos los datos asociados a los servicios utilizados incluida la dirección IP utilizada, por lo que esta tendrá la consideración de dato de carácter personal y le será de aplicación toda la regulación especifica sobre de protección de datos personales.
Por tanto, la Universidad que va a distribuir las direcciones IP es conocedora de la persona a la que le asigna cada dirección o, por lo menos, tiene la posibilidad de identificarla, luego la dirección IP se convierte en un dato de carácter personal que quedará bajo el ámbito de aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Por otra parte, y en la medida que la dirección IP asignada a cada persona esté incorporada a un fichero de datos de carácter personal, dicho fichero deberá estar declarado ante la Agencia de Protección de Datos de la Comunidad de Madrid.

¿Qué requisitos debe cumplir un contrato de prestación de servicios, por ejemplo, de Outsourcing, que una Universidad pretende contratar con una empresa?

La LOPD exige que el contrato que conlleve acceso a datos de carácter personal por cuenta de terceros para prestar un servicio al responsable del fichero, debe formalizarse de manera que se pueda acreditar su celebración y contenido, así como la obligación del encargado del tratamiento de tratar los datos conforme a las instrucciones del responsable, que no se aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas, cumpliendo con los requisitos establecidos por el artículo 12 de la LOPD. Los requisitos de dicho encargo del tratamiento han sido desarrollados por los artículos 20, 21 y 22 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.
A su vez, en el contrato en el que se formalice el encargo se estipularán las medidas de seguridad a que se refiere el artículo 9 de la LOPD y que han sido desarrolladas por el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

¿Puede el Servicio de Biblioteca Universitaria acceder a los datos personales de los alumnos relativos a sus discapacidades o limitaciones para favorecer y mejorar los servicios prestados a dichos alumnos?

El artículo 46.2 b) de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, establece que los Estatutos y normas de organización y funcionamiento desarrollarán los derechos y los deberes de los estudiantes, así como los mecanismos para su garantía. En consecuencia, en los términos establecidos por el ordenamiento jurídico, los estudiantes tendrán derecho a: "La igualdad de oportunidades y no discriminación por razones de sexo, raza, religión o discapacidad o cualquier otra condición o

circunstancia personal o social en el acceso a la universidad, ingreso en los centros, permanencia en la universidad y ejercicio de sus derechos académicos".
Más en concreto, la nueva Disposición adicional vigésima cuarta de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, bajo el título "De la inclusión de las personas con discapacidad en las universidades", dispone que:
"1. Las Universidades garantizarán la igualdad de oportunidades de los estudiantes y demás miembros de la comunidad universitaria con discapacidad, proscribiendo cualquier forma de discriminación y estableciendo medidas de acción positiva tendentes a asegurar su participación plena y efectiva en el ámbito universitario.
2. Los estudiantes y los demás miembros con discapacidad de la comunidad universitaria no podrán ser discriminados por razón de su discapacidad ni directa ni indirectamente en el acceso, el ingreso, la permanencia y el ejercicio de los títulos académicos y de otra clase que tengan reconocidos.
3. Las universidades promoverán acciones para favorecer que todos los miembros de la comunidad universitaria que presenten necesidades especiales o particulares asociadas a la discapacidad dispongan de los medios, apoyos y recursos que aseguren la igualdad real y efectiva de oportunidades en relación con los demás componentes de la comunidad universitaria.
4. Los edificios, instalaciones y dependencias de las universidades, incluidos también los espacios virtuales, así como los servicios, procedimientos y el suministro de información, deberán ser accesibles para todas las personas, de forma que no se impida a ningún miembro de la comunidad universitaria, por razón de discapacidad, el ejercicio de su derecho a ingresar, desplazarse, permanecer, comunicarse, obtener información u otros de análoga significación en condiciones reales y efectivas de igualdad.
Los entornos universitarios deberán ser accesibles de acuerdo con las condiciones y en los plazos establecidos en la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y en sus disposiciones de desarrollo.
5. Todos los planes de estudios propuestos por las universidades deben tener en cuenta que la formación en cualquier actividad profesional debe realizarse desde el respeto y la promoción de los Derechos Humanos y los principios de accesibilidad universal y diseño para todos".
Finalmente, la Disposición adicional cuarta de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, bajo el título Programas específicos de ayuda, establece que:
"Las Administraciones públicas competentes, en coordinación con las respectivas universidades, establecerán programas específicos para que las víctimas del terrorismo y de la violencia de género, así como las personas con discapacidad, puedan recibir la ayuda personalizada, los apoyos y las adaptaciones en el régimen docente".
En consecuencia, de acuerdo con lo dispuesto en la normativa transcrita, el acceso por parte de los Servicios universitarios, y en concreto por parte del Servicio Especial para Discapacitados de una Biblioteca Universitaria, a los datos personales de los discapacitados en orden a la mejor prestación de los servicios que le son propios, tendría amparo en dicha previsión legal, debiendo tenerse en cuenta que, de acuerdo con lo dispuesto en el artículo 4.2 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,"Los datos de carácter personal objeto de tratamiento no podrán utilizarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos". En consecuencia, resultaría ilegítima la utilización de dichos datos por parte del Servicio de Biblioteca para una finalidad distinta a la señalada.

Ello no obstante, el acceso a esta información debe regirse siempre por la obligación de reserva, tal y como disponen los artículos 10 de la LOPD y 11 de la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, cuando regula el deber de secreto para los intervinientes en el tratamiento de los datos.
En conclusión, el Servicio de Biblioteca de una Universidad podrá acceder a los datos personales identificativos de las personas con discapacidad, solicitándolos del Servicio de Alumnos y Planes de Estudios sin previo consentimiento de los afectados cuando dicho acceso sea necesario para la mejora de los servicios ofrecidos en favor de dichas personas.
Ello no obstante, es imprescindible que en la petición efectuada se determine la finalidad del acceso a los datos, así como que se entregue el mínimo de datos necesario de las personas que permitan alcanzar la finalidad pretendida con el acceso.
De igual forma, por el Servicio de Biblioteca no se podrán utilizar los datos a los que acceda para funciones distintas de las previstas en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, en su redacción dada por la reciente Ley Orgánica 4/2007, de 12 de abril.

1.4 Seguridad de los datos

¿Todos los ficheros que contengan datos de carácter personal, ¿deben cumplir las mismas medidas de seguridad?

Las universidades tendrán que implantar las medidas de seguridad adecuadas al grado de protección que requieran los datos contenidos en cada uno de los ficheros, atendiendo a lo dispuesto en el Título VIII, "De las medidas de seguridad en el tratamiento de datos de carácter personal", del Real Decreto 1720/2007, de 21 de diciembre.
Tanto para los ficheros automatizados como para los manuales (ubicados en archivadores, armarios u otros soportes) o mixtos, las medidas de seguridad se clasifican en tres niveles (básico, medio y alto) en función de la naturaleza de la información tratada.
Con carácter general, todos los ficheros manejados por las universidades que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico (sean automatizados, mixtos o manuales). Adicionalmente, todos los ficheros en que se contengan datos de salud, tales como aquellos en los se recoja y conserve información relativa a salud de los estudiantes (vg. fichero de Becas y Ayudas, fichero relativo a salud del personal, fichero de Acción Social, etcétera), deberán implantar medidas de seguridad de nivel alto. Por su parte, los ficheros que recojan datos disciplinarios del personal o de los estudiantes (infracciones administrativas cometidas por los mismos), deberán adoptar medidas de nivel medio.

¿Quién debe ser el responsable de seguridad?

El Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la LOPD, define al responsable de seguridad como la persona que nombrada por el responsable del fichero le ayuda a implantar y controlar las medidas de seguridad. Debe tener la autoridad suficiente para implantar y vigilar el cumplimiento de las medidas de seguridad por parte del resto de los usuarios del fichero.
Normalmente y en relación con los ficheros automatizados, se suele asociar al responsable de seguridad con un perfil técnico, pero dado que muchas de las medidas de seguridad son organizativas, no es un requerimiento imprescindible. En organizaciones complejas y con muchos usuarios, es aconsejable que existan varios responsables de seguridad, un responsable de seguridad para el control y coordinación de las medidas técnicas y uno o varios responsables de seguridad para el control y coordinación de las medidas organizativas de cada área.

¿Qué medidas de seguridad deben aplicarse a un fichero de datos personales informatizado con datos especialmente protegidos ubicado en un único ordenador personal?

Deben aplicarse las medidas que se establecen para los ficheros de nivel alto en el RD 1720/2007, de 21 de diciembre. Entre estas medidas, deberá elaborar un documento de seguridad en el que se recojan las restantes medidas que deberán implantarse. Deberá asimismo designar un Responsable de Seguridad, que deberá controlar el tratamiento de datos que se realice y cumplir las obligaciones que le impone el RD 1720/2007 sin qué, en ningún caso, su designación suponga una delegación de la responsabilidad que corresponde al responsable del fichero.

El ordenador se deberá instalar en un lugar en el que se pueda establecer un control del acceso físico al mismo, no pudiendo estar en zonas comunes o espacios de libre acceso de personas.
Cualquier salida de información del sistema de tratamiento deberá realizarse cifrando los datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte, además debe establecer un sistema de registro de las entradas y salidas de soportes.
Cuando el responsable del fichero sea el único usuario del mismo, y esta circunstancia quedase debidamente acreditada en el documento de seguridad, no será necesaria la implantación del registro de accesos. En el caso de que sean varios los usuarios y no se pueda garantizar la existencia de un sistema de registro de accesos, deberán aplicarse medidas alternativas, como el cifrado de los directorios donde se ubiquen los datos.
Si aún realizando el tratamiento de los datos en un local con acceso restringido, el ordenador personal en el que estén ubicados los datos se conectara a una red de telecomunicaciones, cada transmisión que se realizara por la misma requeriría el cifrado de los datos o la aplicación de cualquier otro mecanismo que garantizase que la información no sea inteligible ni manipulable por terceros. Esta medida no será obligatoria si la red de telecomunicaciones es una red privada.

¿Como debe interpretarse el control de acceso físico?

El control de acceso físico constituye una de las medidas de seguridad de nivel medio cuya implantación se exige por el Real Decreto 1720/2007, de 21 de diciembre, en cuyo artículo 99 se prevé que "Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información".
En relación con dicha cuestión, el consultante apunta dos posibles soluciones, indicando que "la redacción de dicho precepto podría estar haciendo referencia, exclusivamente a los locales donde estén ubicados los servidores (lo que es la sala de ordenadores propiamente dicha)"; y otra más amplia, que entiende que abarca cualquier local en el cual se encuentre ubicado un terminal a través del cual se pueda acceder a datos de carácter personal de ficheros de nivel medio o alto, incluido, por ejemplo, el local en que esté una impresora.
Por su parte, este nuevo Reglamento de desarrollo de la LOPD, en el artículo 2.m), define a los sistemas de información como "conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal".
La regulación establecida en dicho Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, para aplicar las medidas que garanticen un adecuado acceso a los ficheros que contengan datos de carácter personal, se circunscriben a las previsiones contenidas en los artículos 91 y 99 del mismo, en lo referente al establecimiento de controles de acceso y acceso físico para los ficheros sujetos a medidas de nivel básico y medio, y el artículo 103 relativo al registro de acceso a aquellos ficheros sujetos a medidas de nivel alto.
A su vez, el artículo 2.d) del Reglamento define el control de acceso como el "mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos". En estos términos, el artículo 91 se refiere al acceso como cualquier actuación por la que un usuario pueda tener conocimiento directo de "aquellos recursos que precisan para el desarrollo de sus funciones".
Los locales en que se encuentren ubicados los equipos que den soporte a los sistemas de información con datos de carácter personal se considerarán un espacio con acceso restringido y únicamente el personal autorizado en el documento

de seguridad podrá tener acceso. Su delimitación física (una habitación cerrada, una sala de ordenadores, etc.), será la que el responsable de seguridad considere conveniente, siempre y cuando el lugar reúna las necesarias condiciones de seguridad y se realice un control automático o manual del acceso que permita identificar y autorizar el acceso únicamente a las personas definidas en el documento de seguridad.
La consulta plantea cómo debe establecerse el mecanismo de control de acceso físico a los locales donde se encuentren ubicados los equipos sistemas de información, al que se refiere el artículo 99 del Reglamento. En particular, en cuanto al lugar en que debe establecerse el control, deberá ser aquél en que se produzca el acceso material a los ficheros, pudiendo variar desde el propio ordenador central o Host, (en caso de que el fichero pueda ser accesible desde cualquier terminal), los servidores en los que residen los sistemas de información con datos de carácter personal de nivel medio ó alto, a un determinado ordenador personal (en caso de que el fichero sólo se encuentre ubicado en el mismo).
En el caso de los PCs conectados a un HOST o servidor no sería aplicable ese control, puesto que los datos normalmente residen en el servidor o en el Host, salvo que se almacenen en sus discos duros este tipo de datos.
En el caso de las impresoras, hay que prestar especial atención a aquellas en las que se impriman listados masivos con este tipo de datos, como es el caso de la emisión de nóminas y en éste caso serían aplicables los controles de acceso físico. En el caso de la impresión de informes de forma discreta e individual, es decir no masiva, no serían aplicables esos controles, y estas impresoras podrían estar compartidas con otros usuarios, aunque cada usuario debe ser responsable de retirar los documentos lo antes posible, conforme vayan saliendo.

PROCEDIMIENTOS SANCIONADORES

Procedimiento Nº: AAPP/00051/2005

RESOLUCIÓN: R/00346/2006

En el procedimiento de declaración de Infracción de las Administraciones Públicas **AAPP/00051/2005** instruido por la Agencia Española de Protección de Datos a la entidad **COLEGIO PÚBLICO "*ANTONIO ORZA COUTO* "**, vista la denuncia presentada por la **ASOCIACIÓN "*ALBORADA*"** , y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 22/03/2005, tuvo entrada en esta Agencia un escrito firmado por los profesores y profesoras del COLEGIO PÚBLICO "*ANTONIO ORZA COUTO*" (en lo sucesivo el Colegio), en el que declaran que, en una reunión mantenida con la Asociación "*Alborada*" de Madres y Padres de Alumnos del Colegio, han comprobado que ésta dispone de un documento, entregado al Presidente de la citada Asociación por el Director del Colegio, en el que constan sus datos personales. Los profesores acompañan a la denuncia dicho documento denominado "*DOCUMENTO DE ORGANIZACIÓN DEL CENTRO*". En el mismo figuran datos personales relativos a todo el personal del Centro, tales como nombre y apellidos, especialidad, Número de Registro de Personal, antigüedad, domicilio y teléfono.

SEGUNDO: En el marco de las actuaciones previas de investigación practicadas por la Inspección de Datos de esta Agencia para el esclarecimiento de los hechos denunciados, con fecha 6/06/2005, tuvo entrada en esta Agencia un escrito del director del Colegio en el que remite, a requerimiento de esta Agencia, la siguiente información:

"*Con fecha 27/09/2004, la presidenta de la Asociación de Nais e Pais (Madres y Padres) "Alborada" solicitó mediante escrito que se le facilitara a dicha Asociación, entre otras cosas, copia de la Programación General Anual del curso 2004-2005.*

El artículo 73 del Decreto 7/1999, de 7 de enero, por el que se regulan los centros públicos integrados de enseñanzas no universitarias, establece el contenido de la programación general anual. Este Decreto se ha desarrollado por la Instrucción 18 de la Orden de 3 de Octubre de 2000, estableciendo que el "Documento de organización del centro", que forma parte de la programación general anual, es el documento en el que se recogen todos los datos relevantes referidos a aspectos organizativos: horarios de profesores y alumnos, relación de profesores etc.... Dicho documento es remitido a cada Centro por la Inspección educativa y debe ser cumplimentado de acuerdo con las instrucciones que lo acompañan.

Por otra parte, el apartado i) del artículo 86 del Decreto 7/1999, de 7 de enero, establece que las asociaciones de padres y madres podrán, en el ejercicio de sus funciones recibir, entre otros documentos, un ejemplar de la programación general anual.

La entrega del citado documento a la Asociación de Padres y Madres de alumnos "Alborada", se realizó de acuerdo con lo previsto en la legislación vigente".

TERCERO: Con fecha 16/08/2005, la Consejería de Educación e Ordenación Universitaria de la Xunta de Galicia remitió a esta Agencia el modelo de "*Documento de Organización del Centro*" correspondiente al curso 2004-2005, verificándose que los impresos que componen dicho documento son los mismos, que una vez cumplimentados por el Colegio, se entregaron a la Presidenta de la citada Asociación de Padres y Madres del Colegio de conformidad con su solicitud.

CUARTO: A la vista del resultado de las actuaciones previas de investigación, el Director de la Agencia Española de Protección de Datos acordó iniciar, con fecha 16/12/2005, procedimiento de declaración de infracción de las Administraciones

Públicas al Colegio por la presunta infracción del artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.g) de dicha norma. El citado acuerdo fue notificado, según acuse de recibo del Servicio de Correos, con fecha 22/12/2005, sin que dicho Colegio presentara alegaciones al mismo.

QUINTO: En la fase de práctica de pruebas se dieron por reproducidos los documentos incorporados a las actuaciones previas de investigación E/00408/2005.

SEXTO: Terminada la fase de pruebas, el expediente se puso de manifiesto al Colegio, que no presentó alegaciones.

SÉPTIMO: Con fecha 10/05/2006, se emitió Propuesta de Resolución en el sentido de que, por el Director de la Agencia Española de Protección de Datos, se declarase que el Colegio Público "*Antonio Orza Couto*" ha infringido lo dispuesto en el artículo 10 de la LOPD, lo que supone una infracción tipificada como grave en el artículo 44.3.g) de la citada norma.

Notificada dicha Propuesta, el citado Colegio no ha presentado alegación alguna.

HECHOS PROBADOS

PRIMERO: Los profesores del Colegio Público "*Antonio Orza Couto*", han denunciado que el Director del Colegio entregó a la Presidenta de la Asociación "*Alborada*" de Madres y Padres de Alumnos de dicho Colegio el "*DOCUMENTO DE ORGANIZACIÓN DEL CENTRO*", en el que constan los datos personales relativos a todo el personal del Centro, tales como nombre y apellidos, especialidad, Número de Registro de Personal, antigüedad, domicilio y teléfono (folios 1- 127).

SEGUNDO: El Colegio Público "*Antonio Orza Couto*" depende de la Consejería de Educación y Ordenación Universitaria de la Xunta de Galicia y, los impresos que contienen el documento denunciado son los mismos que componen el modelo de "*Documento de Organización del Centro*", correspondiente al Curso 2004-2005 (folios 170-196).

TERCERO: Se ha verificado, que los impresos que componen dicho documento fueron entregados a la Presidenta de la citada Asociación, una vez cumplimentados por el Colegio con los datos personales de los profesores y de todo el personal del Centro (folios 7- 127).

CUARTO: El Director del Colegio ha reconocido que entregó dicho documento a la Presidenta de la Asociación de Madres y Padres "*Alborada*", como consecuencia de la solicitud, que se le hizo por esa Asociación en fecha 27/09/2004, de la copia de la Programación General Anual del Curso 2004-2005 (folios 130-131).

FUNDAMENTOS DE DERECHO

I

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

II

El artículo 10 de la LOPD dispone:

"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."

III

El deber de secreto profesional que incumbe a los responsables de los ficheros, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el*

titular del fichero o, en su caso, con el responsable del mismo". Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, y, por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

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 Constitución Española. En efecto, este precepto contiene un *"instituto de garantía 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"* (Sentencia del Tribunal Constitucional 292/2000). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino 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.

IV

En el presente caso, el Director del Colegio facilitó datos personales de los profesores y de todo el personal del Centro a la Asociación de Madres y Padres "*Aborada*", que no se encontraba habilitada para tener acceso a los mismos. La alegación del Director del Colegio referente a que facilitó dicha documentación de conformidad con la normativa vigente y de acuerdo a un mandato legal no puede ser admitida. En este sentido, cabe señalar que la Orden de 3/10/2000 de la Consejería de Educación y Ordenación Universitaria, relativa a las instrucciones para el desarrollo del Decreto 7/1999, que implanta y regula los centros públicos integrados de enseñanza no universitaria, define en el punto 18 de su Anexo como "*DOCUMENTO DE ORGANIZACIÓN DEL CENTRO*" : " *El documento en el que se recogen todos los datos relevantes referidos a los aspectos organizativos: horarios de profesores y alumnos, relación de profesores, composición de los órganos de gobierno y coordinación docente. Será remitido a cada centro por la Inspección Educativa y debe ser cumplimentado de acuerdo con las instrucciones que le acompañen...".*

Por su parte, el Decreto 7/1999, de 7 de enero, de la Consejería de Educación y Ordenación Universitaria, que implanta y regula los centros públicos integrados de enseñanza no universitaria, establece en su Título V, relativo a "*Asociaciones de padres y madres de alumnos, asociaciones de alumnos y alumnas y otros órganos de participación"* , artículo 86 sobre "*Funciones*", lo siguiente:

"*Estas asociaciones podrán, en el ejercicio de sus funciones:...*

i) Recibir un ejemplar de la programación general anual, del proyecto educativo, de los proyectos curriculares de etapa y de sus modificaciones, así como del reglamento de régimen interior".

Cabe señalar, a este respecto, que si bien se contempla expresamente el derecho de las Asociaciones de Madres y Padres de Alumnos a recibir la "*Programación General Anual*", proyecto educativo y otros proyectos, esto no implica que ello conlleve facilitar y poner en su conocimiento datos personales que van más allá de los datos profesionales y de la actividad en relación con el Centro, no pudiendo, en consecuencia incluir dentro de esa información datos personales de los profesores de dicho Centro, siendo exigible una actuación diligente respecto al tratamiento de la referida información.

En consecuencia, el Colegio ha vulnerado el deber de secreto al enviar a la Asociación de Madres y Padres "*Alborada"* el "*Documento de Organización del Centro*", en el que

se incluían por éste a instancia de la Inspección Educativa, datos personales del personal de dicho Centro.

V

El artículo 44 de la LOPD califica la vulneración del deber de secreto como leve, grave o muy grave, dependiendo del contenido de la información revelada.

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

"La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo".

En el caso que nos ocupa, la información facilitada por el Colegio a la Asociación de Madres y Padres "*Alborada*" contenía varios datos personales del personal del Centro, de lo que cabe deducir que la vulneración del deber de secreto permite realizar una evaluación de la personalidad de los afectados, por lo que, teniendo en cuenta el contenido de la información facilitada, se considera que ha incurrido en la infracción grave descrita.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DECLARAR que el **COLEGIO PÚBLICO *"ANTONIO ORZA COUTO",*** ha infringido lo dispuesto en el artículo 10 de la LOPD, lo que supone una infracción tipificada como grave en el artículo 44.3.g) de la citada Ley Orgánica.

SEGUNDO: REQUERIR al **COLEGIO PÚBLICO *"ANTONIO ORZA COUTO"***, para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 10 de la LOPD.

Las resoluciones que recaigan en relación con las medidas y actuaciones adoptadas, deberán ser comunicadas a esta Agencia Española de Protección de Datos, de acuerdo con el artículo 46.3 de la LOPD. La citada comunicación deberá realizarse en el plazo de un mes.

TERCERO: NOTIFICAR la presente resolución al **COLEGIO PÚBLICO *"ANTONIO ORZA COUTO,"*** 15881 Forte Boqueixón, A Coruña, y a **DOÑA N.D.R.,** (C/.....).

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.

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.

Procedimiento Nº AP/00063/2009

RESOLUCIÓN: R/00604/2010

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00063/2009**, instruido por la Agencia Española de Protección de Datos a las entidades **CONSELLERIA D´EDUCACIÓ DE LA GENERALITAT VALENCIANA (I.E.S. MONSERRAT)** y **UNIVERSIDAD POLITÉCNICA DE VALENCIA**, vista la denuncia presentada por **D. A.A.A.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 02/10/2008, tuvo entrada en esta Agencia Española de Protección de Datos un escrito de D. A.A.A. (en lo sucesivo el denunciante), en el que denuncia a la Universidad Politécnica de Valencia (en lo sucesivo UPV) por insertar en su página web información relativa a su hija, sin su consentimiento, señalando al respecto que dicha información procede del IES Montserrat, del municipio de Montserrat (Valencia), al que pertenecía su hija en la condición de alumna, cuyo Director era D. B.B.B. (en lo sucesivo B.B.B.). Considera que tales datos eran de uso exclusivo por parte del IES Montserrat y que, por tanto, se produce un uso ilegal de los mismos.
En respuesta al requerimiento efectuado por la Inspección de Datos, con fecha 29/01/2009, el denunciante manifestó que los datos personales de su hija se insertaron en la página web de la UPV en el año 2006, aunque no conoció dicha circunstancia hasta el 2008. En relación con los datos divulgados, informó que se incluyeron los relativos a nombre, apellidos, domicilio, fecha de nacimiento, DNI y fotografía del año 2006, así como los datos personales del propio denunciante relativos a domicilio, DNI, teléfono fijo y móvil.
Adjuntó impresión del documento obtenido por él mismo en fecha 23/01/2009, titulado "Gestió del Departament D´Orientació GESDOR", que aparece suscrito por B.B.B. como "Coordinador del proyecte" y corresponde a una presentación de una base de datos de alumnos del centro, que denominan "Programa GESDOR", con indicación de los objetivos, procedimiento de trabajo y estructura del programa, modo de instalación y otra información complementaria.
Dicha herramienta informática incluye los datos personales y académicos del alumno, así como el historial psicopedagógico del estudiante. Asimismo, según se indica en este documento, dicho programa permite obtener automáticamente los datos del programa de gestión de centros de la Consejería de Educación ("GESCEN") y, en relación con los datos personales, añade que se actualizan en función de la matrícula de los alumnos gestionada por la secretaría del Centro.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:
. Con fecha 14/04/2009, los Servicios de Inspección de la Agencia Española de Protección de Datos accedieron a la dirección de Internet "upv.es/", obteniendo el documento "Gestió del Departament D´Orientació GESDOR" en formato "pdf" y constatando que la información relativa al denunciante y a su hija era de libre acceso.
. En respuesta al requerimiento de información efectuado por la Inspección actuante en relación con los hechos denunciados, la UPV manifestó lo siguiente:
. Los datos personales relativos al denunciante y su hija a los que se accede a través de la dirección de Internet "upv.es/ " se encuentran reflejados en la comunicación

titulada “Gestió del Departament D’Orientació GESDOR” que B.B.B. realizó al I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por el Área de Información de la UPV en el año 2006.
. B.B.B., que se registró como ponente de dicho congreso el 10/10/2006, realizó el envío de la indicada comunicación, que fue publicada con el resto de ponencias del congreso del día 19/10/2006, manteniéndose publicada hasta que la Universidad tuvo conocimiento, tras recibir la llamada del denunciante el 05/03/2009, de que existía la posibilidad de que esta publicación infringiese el derecho a la protección de datos personales de su hija, retirándose inmediatamente y de forma preventiva la citada comunicación.
. No consta a la UPV que B.B.B. tenga consentimiento del denunciante y su hija para el tratamiento de sus datos. La UPV, por su parte, se ha limitado a publicar en la web los trabajos facilitados por los autores, sin hacer ningún tratamiento posterior de los datos que puedan estar incluidos en los mismos, y entiende que el autor de la ponencia debe haber cumplido con la legalidad vigente.

TERCERO: Con fecha 28/09/2009, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a la entidad Conselleria D´Educació de la Generalitat Valenciana, por las presuntas infracción del artículo 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como muy grave en los artículos 44.4.b), y a la entidad UPV por las presuntas infracciones de los artículos 6 y 10 de la misma norma, tipificadas como leve y grave en los artículos 44.2.e) y 44.3.d), respectivamente, de la citada Ley Orgánica.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, se recibe escrito del denunciante, de fecha 22/10/2009, en el que solicita se le tenga por personado en el procedimiento, Por su parte, la entidad Conselleria D´Educació de la Generalitat Valenciana presentó escrito de alegaciones en el que manifiesta que la denuncia se formula contra la Universidad Politécnica de Valencia (UPV) por unos hechos de su exclusiva responsabilidad, relacionados con la inserción en su página web, sin conocimiento del denunciante, de determinada información relativa a la hija de éste.
En cuanto a cesión de los datos por parte del IES de Montserrat a la citada Universidad, admite que los datos de los usuarios del servicio público educativo que integran el fichero están destinados única y exclusivamente a las tareas inherentes al funcionamiento del centro docente y no cabe hablar, en ningún caso, de un supuesto en que esté permitida la comunicación o cesión de datos, pero advierte que no ha quedado acreditado que dicha cesión se haya efectuado por parte de la Consellería d'Educació de la Generalitat Valenciana (ÍES de Montserrat), y añade que consta expresamente que B.B.B. "realizó el envío de la citada documentación", actuando en su condición de ponente en el I Congrés d'Innovació en Orientació per a la Universitat, organizado por el Área de Información de la UPV, y no como director del citado Instituto.
Tales ponencias son presentadas "exclusivamente por profesores de enseñanzas universitarias". No se trata, por tanto, de una representación institucional de la Consellería d'Educació, ni aún del ÍES de Montserrat, sino de un profesor de enseñanza secundaria que, si bien ocasionalmente desempeñaba el puesto de trabajo de director, participa en una actividad a título exclusivamente personal, al margen de las funciones que tiene encomendadas de acuerdo con la normativa relativa a la organización y funcionamiento de los centros docentes y, por consiguiente, bajo su exclusiva responsabilidad, como resulta obvio del hecho que la administración educativa no interviene ni supervisa la ponencia.

Por otra parte, el plazo concedido a la entidad UPV para formular alegaciones, de quince días a contar desde la notificación de la apertura del procedimiento, que tuvo lugar el 02/10/2009, transcurrió sin que se recibiera escrito alguno de la misma.

QUINTO: En fecha 24/11/2009, se acordó por el Instructor del procedimiento la apertura del período de pruebas, teniéndose por reproducidas las actuaciones previas de investigación desarrolladas por los Servicios de Inspección, señaladas con el número E/01977/2008, e incorporada la documental aportada por el denunciante con su escrito de denuncia. Asimismo, se tuvieron por presentadas las alegaciones formuladas por la entidad Conselleria D´Educació de la Generalitat Valenciana a la apertura del presente procedimiento y por presentada la documentación aportada por dicha entidad con su escrito de alegaciones.

Asimismo, por el Instructor del procedimiento se acordó incorporar a las actuaciones el resultado de la consulta efectuada al Registro General de Protección de Datos sobre ficheros inscritos en el mismo cuya titularidad corresponda a la Conselleria D´Educació de la Generalitat Valenciana, comprobándose que dispone, entre otros, de unos ficheros denominados "Alumnos" y "Alumnos extendido". Según consta en la inscripción respectiva, el fichero "Alumnos" tiene como finalidad y usos previstos la "admisión, matriculación, controles de asistencia, expedición de títulos y diplomas académicos, gestión de comedor y transporte escolar, atención a la diversidad", y el fichero "Alumnos extendido" tiene como finalidad y usos previstos "datos sanitarios de alumnos/as con necesidades especiales, datos sanitarios de alumnos/as necesarios para los regímenes de comidas, traslados, necesidades educativas especiales (informes psicopedagógicos) y requerimientos sanitarios específicos".

Por otra parte, en atención a lo solicitado por la Conselleria D´Educació de la Generalitat Valenciana, se remitió a la misma copia de las actuaciones previas de investigación que determinaron la apertura del presente procedimiento, que incorporan la denuncia formulada, y se le concedió un plazo para formular propuesta de prueba. Así, con fecha 16/12/2009, tuvo entrada en esta Agencia un escrito de la citada Conselleria en el que solicita que se practique prueba testifical, para que por B.B.B. se respondan las siguientes cuestiones:

"1. Su participación en el I Congreso de Innovación y Orientación para la Universitat Politècnica de Valéncia (UPV) ¿se produjo a título personal, sobre la base de su cualificación profesional o en representación oficial de la Conselleria de Educación de la Generalitat?

2. ¿Recibió instrucciones de alguna instancia de la Conselleria de Educación en orden a intervenir en dicho Congreso?

3. ¿Recibió instrucciones en orden a aportar a dicho Congreso los datos en cuestión?

4. ¿Conoce que los funcionarios públicos tienen deber de secreto respecto de las materias cuya difusión está prohibida legalmente?".

En respuesta al requerimiento efectuado por el Instructor, B.B.B. comunicó lo siguiente:

"1.- La participación en los Congresos y Jornadas de Orientación que organizan las universidades valencianas, la inscripción siempre se realiza a título personal. En este Congreso, en relación con la temática del mismo, presenté un proyecto de investigación e innovación educativa que, por su interés general y aplicabilidad, fue seleccionado y subvencionado en la resolución de 18 de octubre de 2005 de la Dirección General de Enseñanza.

El objetivo de este proyecto "Programa de Gestión para el Departamento de Orientación. GESDOR" es la creación de una herramienta, a modo de base de datos, para facilitar a los psicopedagogos de los centros educativos su tarea profesional.

Para explicar el programa informático GESDOR utilizamos datos ficticios o inconexos, y lógicamente son los propios psicólogos de los centros quienes introducen sus contenidos propios.

Los datos utilizados para explicar esta herramienta, siempre han sido ficticios y aleatoriamente inconexos. En la ponencia antes citada, siempre se utilizaron datos irreales, quizás en algunos casos puntuales podía haberse dado de manera fortuita una coincidencia casual entre datos de ubicación, como por ejemplo que coincida el nombre de la persona y la población donde reside, datos que podemos encontrar en cualquier guía telefónica.
Revisando el texto publicado en las actas del CÍES 2006 sólo encuentro el dato de un padre y su hija que podría dar lugar a confusión, no obstante se trata de una familia con la que manteníamos una cordial amistad y conocían el desarrollo del programa de innovación educativa, y en su momento no hubo ningún problema al respecto.
Insisto, nunca ni bajo ninguna circunstancia se utilizaron datos de historiales clínicos, ni de entrevistas, y esta afirmación la pueden avalar todos los miembros del equipo de trabajo y todos los profesionales de la psicología que hoy utilizan el programa GESDOR para su gestión del departamento de orientación.
2.- No. Entiendo que no procedía ninguna instrucción específica por parte de dicha Conselleria, pues en este primer congreso se trataba de compartir experiencias de innovación educativa entre los profesionales del sector, y que finalmente se resumió en unas actas.
3.- No. El objetivo de la ponencia en dicho congreso no era aportar datos, sino la explicación del funcionamiento de un programa informático GESDOR, lógicamente fue necesario introducir datos, todos ellos ficticios.
En ningún momento la Consellería de Educación intervino en el proceso de intercambio de los trabajos de investigación e innovación educativa que se presentaron en dichas jornadas.
4.- Efectivamente lo conozco y lo practico. Desde hace 16 años ejerzo la tarea profesional de psicólogo y trabajador público. Han pasado por mi despacho diversos y complejos casos, y siempre he guardado el secreto profesional actuando con honradez, respeto y coherencia. Conozco perfectamente la normativa que regula la protección de datos, y bajo ningún concepto he pretendido infringirla ni sortearla".

SEXTO: Mediante escrito fechado el 04/12/2009, la entidad UPV, en respuesta a la notificación del período de pruebas que le fue realizada por el Instructor del procedimiento, manifiesta no tener conocimiento de la apertura del procedimiento de declaración de infracción de las Administraciones Públicas de referencia. En respuesta a dicho escrito, se remitió a la misma copia del acuerdo de inicio respectivo, que fue notificado a esa Universidad en fecha 02/10/2009, según consta en el correspondiente aviso de recibo. Asimismo, se advirtió a dicha entidad que el procedimiento se rige por el principio de acceso permanente, conforme a lo dispuesto en el artículo 3 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, por lo que en cualquier momento podrá conocer su estado de tramitación, acceder y obtener copia de los documentos contenidos en el mismo y formular alegaciones, con anterioridad al trámite de audiencia.

SÉPTIMO: Con fecha 17/02/2010, se emitió propuesta de resolución en el sentido de que por el Director de la Agencia Española de Protección de Datos se declare que la entidad UPV ha infringido lo dispuesto en el artículo 6 de la LOPD, lo que supone una infracción tipificada como grave en el artículo 44.3.d) de dicha norma, y que se acuerde el archivo de las actuaciones seguidas contra la Conselleria D´Educació de la Generalitat Valenciana por la presunta infracción de lo dispuesto en el artículo 11.1 de la LOPD.
Notificada dicha propuesta, la entidad UPV presenta escrito de alegaciones en el que manifiesta que la misma desconocía que los datos personales incluidos en el proyecto

de B.B.B., avalado y subvencionado por la Generalitat Valenciana, pertenecieran a personas físicas determinadas, por lo que no entendió que pudiera lesionar ningún derecho de terceros con la publicación de la comunicación presentada por aquél al Congreso. Así, tratándose de un proyecto de innovación educativa que había sido revisado por la Generalitat Valenciana, que además, según consta en la convocatoria de ayudas respectiva, se reservaba los derechos de reproducción, distribución, comunicación pública y traducción durante un año, se estimó que dicho proyecto cumplía con la legalidad vigente. La utilización de datos ficticios consta, asimismo, en la testifical de B.B.B.. En definitiva, queda acreditado que la UPV no era consciente de estar cometiendo una infracción.

Por otra parte, señala que el proyecto citado se presentó al Congreso por la persona que, en aquel momento, era Director del IES Monserrat responsable de los datos de los afectados, y que éste conocía que tales datos únicamente pueden utilizarse con fines educativos, conforme a la disposición adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, por la que la UPV consideró que de tratarse de datos reales el Director del Instituto habría recabado el consentimiento de los afectados.

Añade que la responsabilidad por cesión de los datos debe imputarse a título de culpa o negligencia al titular del fichero, en el presente caso, la Conselleria D´Educació de la Generalitat Valenciana, no correspondiendo a la entidad cesionaria verificar el consentimiento previo de los interesados para la cesión, según se declara en la Sentencia de la Audiencia Nacional de 30/06/2004, en la que se declara lo siguiente:

"Por lo demás, tal posibilidad de que el cesionario lesione el principio del consentimiento cuando trata y utiliza datos cedidos sin que se haya obtenido el previo consentimiento ha sido ya estudiado y resuelto por esta Sala y Sección, en sentido afirmativo, en la sentencia de 15 de septiembre de 2001 dictada en el recurso 1120/1999 en la que, entre otros razonamientos exponíamos que, si bien no puede serle exigido al cesionario la obtención del previo consentimiento de los datos cedidos, pues tal obligación es del cedente, sí debe serle exigido, conforme a parámetros de razonable diligencia en el mercado de tráfico de datos, que verifique en forma diligente que dicho consentimiento ha sido obtenido. En caso contrario, cuando dolosamente conozca que dicho consentimiento no ha sido obtenido; o no realice una actividad razonable y diligente tendente a verificar la existencia de dicho conocimiento incurriendo en negligencia o culpa, se produce una lesión del principio del consentimiento, pues el cesionario usa de datos, en los que por dolo o culpa no le consta la existencia del previo consentimiento, y por lo tanto trata datos en contra de lo manifestado por la persona titular de los datos, con lesión de su privacidad".

A la vista de esta Sentencia, la UPV considera que la entidad que recibe los datos debe realizar "una actividad razonable y diligente tendente a verificar la existencia de dicho consentimiento", estableciendo que para que pueda imputársele una infracción debe mediar dolo o culpa por parte de dicha entidad y, en el presente caso, por las circunstancias antes expresadas, resulta razonable que la Universidad estimar que el Director del Instituto hubiese obtenido el consentimiento o que los datos utilizados por el mismo fueran ficticios. En base a ello, la UPV invoca el principio de culpabilidad.

Asimismo, señala que, en cualquier caso, los datos en cuestión han sido utilizados con fines científicos, habiéndose limitado el tratamiento a la publicación de la comunicación presentada por B.B.B., ajustado a las funciones específicas atribuidas a la Universidad y conforme con lo establecido en el artículo 10 del Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de desarrollo de la LOPD, que admite el tratamiento de datos sin necesidad del consentimiento del interesado cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de las competencias que una norma con rango de ley o norma de derecho comunitario les atribuya.

Finalmente, manifiesta que se procedió a retirar el documento en cuanto tuvo conocimiento de la protesta del afectado y que este cese en el tratamiento ha sido valorado en otras ocasiones por la Agencia Española de Protección de Datos para fundamentar el archivo de las actuaciones (E/00595/2008 y E/01220/2007).

OCTAVO: Con fecha 11/03/2010, el denunciante formuló alegaciones la propuesta de resolución, señalando que su denuncia se formuló contra B.B.B., que ha seguido utilizando el "Programa GESDOR", según acredita mediante un documento correspondiente a la presentación de dicho programa en una Jornadas en febrero de 2008 en el IES Tirant Lo Blanc, al que considera responsable de una infracción muy grave cuya prescripción hubiera tenido lugar en fecha 19/10/2009, posterior a la apertura del procedimiento. En cualquier caso, añade que la infracción que resulta de la utilización de los datos en la citada presentación del programa celebrada en 2008 no ha prescrito.
Asimismo, manifiesta que la actuación de la UPV retirando el documento de su Web en tres horas ha sido impecable.

HECHOS PROBADOS

PRIMERO: La Conselleria D´Educació de la Generalitat Valenciana, entre otros, dispone de unos ficheros denominados "Alumnos" y "Alumnos extendido". Según consta en la inscripción respectiva, el fichero "Alumnos" tiene como finalidad y usos previstos la "admisión, matriculación, controles de asistencia, expedición de títulos y diplomas académicos, gestión de comedor y transporte escolar, atención a la diversidad", y el fichero "Alumnos extendido" tiene como finalidad y usos previstos "datos sanitarios de alumnos/as con necesidades especiales, datos sanitarios de alumnos/as necesarios para los regímenes de comidas, traslados, necesidades educativas especiales (informes psicopedagógicos) y requerimientos sanitarios específicos".

SEGUNDO: En el año 2006, la hija del denunciante figuraba como alumna del IES Montserrat (Valencia), adscrito a la Conselleria D´Educació de la Generalitat Valenciana, del que era Director B.B.B..

TERCERO: B.B.B., actuando como coordinador del proyecto, dirigió un grupo de trabajo que tuvo por objeto la elaboración de un programa informático, denominado "Programa GESDOR", que permite obtener automáticamente los datos del programa de gestión de centros de la Consejería de Educación ("GESCEN") y actualizarlos en función de la matrícula de los alumnos gestionada por la secretaría del Centro de que se trate, elaborando una base de datos que incluye los datos personales y académicos del alumno, así como el historial psicopedagógico del estudiante.
Relacionado con este proyecto, B.B.B. elaboró un documento titulado "Gestió del Departament D ´Orientació GESDOR", que aparece suscrito por el mismo como "Coordinador del proyecte" y corresponde a una presentación del "Programa GESDOR", con indicación de los objetivos, procedimiento de trabajo y estructura del programa, modo de instalación y otra información complementaria. En este documento se incluyeron los datos personales de la hija del denunciante relativos a nombre, apellidos, domicilio, fecha de nacimiento, DNI y fotografía del año 2006, como alumna de 4º curso de ESO, así como los datos personales del propio denunciante relativos a domicilio, DNI, teléfono fijo y móvil.

CUARTO: En el año 2006, la UPV celebró el I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por el Área de Información de dicha Universidad.

QUINTO: Con fecha 10/10/2006, B.B.B. se registró, a título personal, como ponente del I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por la UPV. Con este motivo, B.B.B. remitió a la UPV el documento titulado "Gestió del Departament D ´Orientació GESDOR", que fue insertado por ésta en su página web el día 19/10/2006, con el resto de ponencias del congreso. Dicho documento permaneció accesible para terceros en la dirección de Internet "upv.es/".

SEXTO: Con fecha 14/04/2009, los Servicios de Inspección de la Agencia Española de Protección de Datos accedieron a la dirección de Internet "upv.es/", obteniendo el documento "Gestió del Departament D´Orientació GESDOR" en formato "pdf" y constatando que la información relativa al denunciante y a su hija era de libre acceso.

SÉPTIMO: B.B.B. ha reconocido que realizó a título personal la inscripción como ponente en el I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por el Área de Información de la UPV en el año 2006, y que no recibió instrucciones de la Conselleria D ´Educació de la Generalitat Valenciana en relación con su participación en el citado Congreso y que dicha Consellería *"En ningún momento ... intervino en el proceso de intercambio de los trabajos de investigación e innovación educativa que se presentaron en dichas jornadas".*

FUNDAMENTOS DE DERECHO

I

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

II

El artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"*.

En cuanto al ámbito de aplicación de la citada norma el artículo 2.1 de la misma señala:
"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado". Perfilándose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la citada LOPD, en el que se define como: *"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, 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. El tratamiento de datos se define en la letra c) del mismo precepto como las *"Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación,*

conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

III

Se imputa a la UPV la vulneración del artículo 6 de la LOPD, por insertar en su página web, accesible a terceros, el documento titulado "Gestió del Departament D´Orientació GESDOR", correspondiente a la ponencia elaborada por B.B.B. para participar en el I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por el Área de Información de la UPV en el año 2006, en los que se reseñan los datos personales de la hija del denunciante relativos a nombre, apellidos, domicilio, fecha de nacimiento, DNI y fotografía del año 2006, como alumna de 4º curso de ESO, así como los datos personales del propio denunciante relativos a domicilio, DNI, teléfono fijo y móvil. Se analiza, por tanto, un tratamiento de datos consistente en incorporar a una página web un documento en el que figuran datos personales de los afectados sin haber procedido a la debida anonimización de dicho documento. En orden a precisar el alcance antijurídico de los referidos hechos respecto de la UPV, procede analizar el principio de consentimiento consagrado en el artículo 6.1 y 2 de la LOPD, que establecen lo siguiente,

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30/11 (FJ. 7 primer párrafo)… "*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

El tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.

Así, para que el tratamiento de datos efectuado por parte de la UPV resultara conforme con los preceptos de la LOPD hubieran debido concurrir en el supuesto

examinado los requisitos contemplados en el artículo 6 de la mencionada norma. Sin embargo, en el presente caso, dicha Universidad no ha acreditado disponer del preceptivo consentimiento prestado al efecto por los titulares de los datos.
Este hecho supone un tratamiento de datos de carácter personal sin consentimiento del afectado. A este respecto, debe reiterarse lo establecido en el artículo 3.c) de la LOPD, que define el tratamiento de datos como las *"Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"*.
Por tanto, al no concurrir ninguno de los supuestos del artículo 6.2 de la LOPD que permiten excepcionar la obtención del consentimiento para el tratamiento de datos, se concluye que la actuación de la UPV constituye una vulneración al repetido artículo 6.1 de la LOPD.
Esta interpretación coincide con la mantenida por el Tribunal de Justicia de las Comunidades Europeas en sentencia de 6 de noviembre de 2003, dictada en el asunto C-101/01, Caso Lindqvist, en el que se examina la aplicación de la Directiva 95/46/CE a un tratamiento consistente en publicar datos personales en Internet. Esta Sentencia, en sus apartados 24 y siguientes, señala:
"24. El concepto de "datos personales" que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva "toda información sobre una persona física identificada o identificable". Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones.
25. En cuanto al concepto de "tratamiento" de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales". Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole.
26. Queda por determinar si dicho tratamiento está "parcial o totalmente automatizado". A este respecto, es preciso observar que difundir información en una página web implica, de acuerdo con los procedimientos técnicos e informáticos que se aplican actualmente, publicar dicha página en un servidor, así como realizar las operaciones necesarias para que resulte accesible a las personas que están conectadas a Internet. Estas operaciones se efectúan, al menos en parte, de manera automatizada.
27. Por tanto, procede responder a la primera cuestión que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46".
Por otra parte, procede citar la Sentencia de la Audiencia Nacional de fecha 21/12/2001 en la que declara que *"de acuerdo con el principio que rige en materia probatoria (art. 1214 del Código Civil) la Agencia de Protección de Datos probó el hecho constitutivo que era el tratamiento automatizado de los datos personales de D. ... (nombre, apellidos y domicilio), y a la recurrente incumbía el hecho impeditivo o extintivo, cual era el consentimiento del mismo. Es decir, ... debía acreditar el consentimiento del afectado para el tratamiento automatizado de datos personales, o justificar que el supuesto examinado concurre alguna de las excepciones al principio*

general del consentimiento consagrado en el art. 6.1 de la Ley Orgánica 5/1992. Y nada de esto ha sucedido".

Por tanto, corresponde a la UPV acreditar que cuenta con el consentimiento de los afectados para el tratamiento de sus datos personales. Sin embargo, en el supuesto examinado, consta acreditado que la citada entidad no realizó actividad alguna para asegurarse de que los datos se utilizaron con el consentimiento de los afectados, resultando, por tanto, evidente la existencia de, al menos, una falta de la diligencia debida en los hechos imputados plenamente imputable a dicha entidad, que trató los datos del denunciante sin su consentimiento.

Dicha actitud negligente se constata, igualmente, a la vista de las alegaciones realizadas por la UPV, en las que señala que las circunstancias concurrentes le permitieron suponer que el autor del documento insertado en su Web habría recabado el consentimiento de los afectados o que desconocía la utilización de datos pertenecientes a personas determinadas, a pesar de resultar evidente que algunos datos, como la fotografía de alumnos, eran reales. A este respecto, la misma Sentencia de la Audiencia Nacional invocada por la Universidad declara negligente, en supuestos de cesión de datos, el tratamiento de los mismos realizado por la entidad cesionaria sin haber realizado una mínima actividad tendente a verificar la existencia del consentimiento del interesado. En dicha Sentencia se declara, según ha quedado expuesto, lo siguiente:

"... si bien no puede serle exigido al cesionario la obtención del previo consentimiento de los datos cedidos, pues tal obligación es del cedente, sí debe serle exigido, conforme a parámetros de razonable diligencia en el mercado de tráfico de datos, que verifique en forma diligente que dicho consentimiento ha sido obtenido. En caso contrario, cuando dolosamente conozca que dicho consentimiento no ha sido obtenido; o no realice una actividad razonable y diligente tendente a verificar la existencia de dicho conocimiento incurriendo en negligencia o culpa, se produce una lesión del principio del consentimiento, pues el cesionario usa de datos, en los que por dolo o culpa no le consta la existencia del previo consentimiento, y por lo tanto trata datos en contra de lo manifestado por la persona titular de los datos, con lesión de su privacidad".

Lo expuesto tiene relación con el principio de culpabilidad invocado por UPV, procediendo considerar lo establecido en 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 (en lo sucesivo LRJPAC), según el cual *"... sólo 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, pues la doctrina del Tribunal Constitucional (Sentencias de 26/04/1990, 19/12/1991 y 04/07/1999, entre otras) y la jurisprudencia mayoritaria del Tribunal Supremo (Sentencia de 23/01/1998, entre otras), así como las exigencias inherentes a un Estado de Derecho, exigen que el principio de culpabilidad requiera la existencia de dolo o culpa.

El Tribunal Supremo (Sentencias de 16 y 22/04/1991) 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*."

Por su parte, la Audiencia Nacional, en Sentencia de 29/06/2001, 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..."*.

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. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor, etc. En este sentido la Sentencia de 05/06/1998 exige a los profesionales del sector *"... un deber de conocer especialmente las normas aplicables".* En similares términos se pronuncian las Sentencias de 17/12/1997, 11/03/1998, 02/03 y 17/09/1999.

Aplicando la anterior doctrina, la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14/02/ y 20/09/2002 y 13/04/2005, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

Conforme a esta doctrina jurisprudencial, es evidente la existencia en este caso de, al menos, una falta de diligencia debida que le era exigible en los hechos denunciados atribuible plenamente a la entidad UPV de acuerdo con las circunstancias antes expresadas.

Finalmente, considera la citada entidad que, en cualquier caso, el tratamiento de datos realizado no requiere el consentimiento de los afectados al haberse realizado en ejercicio de las funciones atribuidas a una Administración Pública y con fines científicos. Sin embargo, en el caso presente, el tratamiento de datos no se realiza en el marco de un proyecto "científico" desarrollado por dicha Institución. Además, la utilización de datos personales en proyectos de esa naturaleza está subordinada a los principios de calidad de los datos y de proporcionalidad establecidos en la LOPD, que obligan a valorar las circunstancias que concurren en cada caso.

Así el artículo 4 de la misma establece en su apartado primero que *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*. En el supuesto analizado, el documento insertado en la Web de la UPV tenía por finalidad presentar el "Programa GESDOR" y es obvio que para ello no era necesario la utilización de los datos personales de los afectados.

IV

La publicación en la Web de la UPV de los datos del denunciante y su hija, según ha quedado indicado, posibilita el acceso a dichos datos personales por parte de terceros. Por tanto, procede analizar, igualmente, el cumplimiento por la citada UPV del deber de secreto establecido en el 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 comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo". Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente no pueden ser conocidos por ninguna persona o entidad

ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.
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 riego 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 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). Este derecho fundamental a la protección de datos 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.
En el presente supuesto la UPV vulnera el deber del secreto de los datos personales del denunciante y su hija que figuran en el documento "Gestió del Departament D´Orientació GESDOR" insertado en el sitio web www.upv.es de la citada Universidad, por cuanto dicho deber comporta que los datos que han sido recogidos o tratados para un determinado fin no sean divulgados a terceras personas totalmente ajenas a la relación en la que los datos fueron recogidos. Atendiendo a la naturaleza de los datos divulgados, la infracción del deber de secreto se ajusta al tipo establecido en el artículo 44.2.e) de la LOPD, que tipifica como infracción leve *"incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave"*.

V

Se comprueba que un mismo hecho, insertar en la web de la UPV los datos señalados, con indicación del nombre, apellidos, domicilio, fecha de nacimiento, DNI, fotografía, teléfono fijo y móvil, da lugar a las dos infracciones reseñadas, dándose la circunstancia que la comisión de una implica necesariamente la comisión de la otra.
A este respecto, debe considerarse lo dispuesto en 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, según el cual cuando de la comisión de una infracción derive necesariamente la comisión de otra, se impondrá únicamente la sanción correspondiente a la infracción más grave. En este caso, procede imponer la sanción prevista por el incumplimiento del artículo 6 por tratarse de la infracción determinante de la otra y por tratarse de la infracción más grave.
Por lo tanto, aplicando el artículo 4.4 del citado Real Decreto 1398/1993, procede subsumir ambas infracciones en una. Dado que, en este caso, ambas infracciones están tipificadas como graves, se considera que procede imputar únicamente la infracción del artículo 6.1 de la LOPD.

VI

El artículo 44.3.d) de la LOPD considera infracción grave: "*Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave".*
La Audiencia Nacional ha manifestado, en su Sentencia de 22/10/03, que *"la descripción de conductas que establece el artículo 44.3d) de la Ley Orgánica 15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave "tratar de forma*

automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley", por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizadamente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos, realizando envíos publicitarios."
La Sentencia de la Audiencia Nacional, de fecha 27/10/04, ha declarado: *"Sucede así que, como ya dijimos en la Sentencia de 8 de octubre de 2003 (recurso 1821/01) el mencionado artículo 44.3 d) de la Ley Orgánica 15/1999, aún no siendo, ciertamente, un modelo a seguir en lo que se refiere a claridad y precisión a la hora de tipificar una conducta infractora, no alberga una formulación genérica y carente de contenido como afirma la demandante. La definición de la conducta típica mediante la expresión "tratar los datos de carácter personal..." no puede ser tachada de falta de contenido pues nos remite directamente a cualquiera de las concretas actividades que el artículo 3.d) de la propia Ley incluye en la definición de "tratamiento de datos" (recogida, grabación, conservación, elaboración, ... de datos de carácter personal). Y tampoco cabe tachar de excesivamente genérico o impreciso el inciso relativo a que el tratamiento o uso de los datos se realice "... con conculcación de los principios y garantías establecidos en la presente Ley...", pues tales principios y garantías debidamente acotados en el Título II del propio texto legal bajo las rúbricas de Principios de la Protección de Datos (artículos 4 a 12) y Derechos de las Personas (artículos 13 a 19)"*.
En este caso, UPV ha incurrido en la infracción descrita ya que ha vulnerado dicho principio, consagrado en el artículo 6.1 de la LOPD, al tratar los datos de los afectados sin su consentimiento.
La descripción de conductas que establece el artículo 44.3.d) de la LOPD cumple las exigencias derivadas del principio de tipicidad, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. El tipo aplicable considera infracción grave *"tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley"*, por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la LOPD. El principio del consentimiento se configura como principio básico en materia de protección de datos y así se recoge en la doctrina y jurisprudencia de los Tribunales Ordinarios como del Tribunal Constitucional en Sentencia 292/2002 y en números Sentencias de la Audiencia Nacional, entre otras, las de fechas 25/05/01 y 05/04/02.
Concretamente, por lo que ahora interesa, el artículo 6 de la LOPD recoge el citado principio que exige la necesidad de consentimiento de los afectados para que puedan tratarse sus datos de carácter personal, salvo en los casos a que se refiere su apartado 2.
Por tanto, UPV vulnera el citado principio, toda vez que ha quedado acreditado el tratamiento de los datos personales de los afectados, al publicarlos en la referida página web sin su consentimiento.

VII

Por otra parte, en el presente supuesto se imputa a la Conselleria D´Educació de la Generalitat Valenciana por la cesión a terceros de los datos personales registrados en sus ficheros de alumnos, que resulta de la entrega a la UPV del documento "Gestió del Departament D´Orientació GESDOR", en el que se contienen los datos del denunciante y de su hija, alumna de un instituto adscrito a la citada Consellería.

El artículo 11.1 y 2 de la LOPD dispone lo siguiente: *"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"*. La LOPD define, en su artículo 3.i), la *"cesión o comunicación de datos"* como *"toda revelación de datos realizada a una persona distinta del interesado"*, y el Real Decreto 1332/1994, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, considera cesión de datos *"toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada"*.

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 personales y a la libre circulación de estos datos, se refiere en su artículo 2.b) a la cesión, dentro de la definición del tratamiento de datos, y la define como *"comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso de los datos, cotejo o interconexión"*.

Por otra parte, el artículo 10 de la LOPD 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"*.

Debe compararse el texto de los artículos 10 y 11 de la LOPD, que definen, respectivamente, los deberes de secreto profesional respecto de los datos de carácter personal que integran el fichero y la prohibición de comunicación, salvo los supuestos previstos, de dichos datos, pues la trasgresión de cualquiera de dichas garantías por parte de quien se responsabiliza del fichero supone, desde un punto de vista meramente fáctico, una conducta semejante: la comunicación de la información que se contiene en el fichero. Así, la distinción entre ambos tipos de garantías exige que la cesión suponga un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados de forma automatizada por parte del cesionario, en este caso la UPV, circunstancia que no concurre en este caso, por lo que la comunicación acontecida debe encuadrarse dentro del marco del deber de secreto recogido en el artículo 10 de la LOPD.

La LOPD califica la vulneración del deber de secreto como infracción leve, grave o muy grave, dependiendo del contenido de la información facilitada al tercero. Así, el artículo 44.2.e) de dicha Ley Orgánica califica como infracción leve *"Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave"*.

Tal incumplimiento sólo constituye una infracción grave en los casos específicamente enunciados en el artículo 44.3.g) de la LOPD, es decir, cuando la vulneración del deber de guardar secreto afecte a *"... los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo"*.

Así, en el presente caso, de acuerdo con lo expuesto, se considera que se vulneró el deber de secreto al comunicar los datos referentes a nombre, apellidos, domicilio, fecha de nacimiento, DNI, fotografía, teléfono fijo y móvil. Se trata de una información que no permite realizar una evaluación de la personalidad del mismo, de modo que se considera que se incurrió en la infracción leve anteriormente descrita.
Por tanto, resulta oportuno valorar el tiempo transcurrido desde que se cometió la infracción de aquel precepto, considerando que la revelación de los datos de los afectados es anterior al 19/10/2006, fecha en la que el documento "Gestió del Departament D´Orientació GESDOR" fue insertado en el sitio web www.upv.es. A este respecto el artículo 47 de la LOPD establece lo siguiente:
"1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.
2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor". Por otra parte, como señala el artículo 132.2 de la LRJPAC, *"El plazo de prescripción de las infracciones comenzará a contarse desde el día que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador"*.
En consecuencia, la presunta infracción del precepto antes citado, calificada como leve, ya había prescrito cuando se formuló la denuncia ante esta Agencia Española de Protección de Datos (02/10/2008), por el transcurso de más de un año desde que el momento en el que pudo cometerse dicha infracción.
En cualquier caso, en el presente procedimiento, si bien ha quedado acreditado que la UPV tuvo acceso a los datos de los afectados y que tales datos procedían de los ficheros de alumnos de la Conselleria D´Educació de la Generalitat Valenciana, ha de tenerse en cuenta que, la Consellería imputada no intervino en la revelación de tales datos a la UPV, que fue llevada a cabo por parte de B.B.B., que pudo acceder a los mismos por su condición de director del instituto en el que cursaba estudios la hija del denunciante y los utilizó para la presentación de un programa informático que permitía la elaboración de una base de datos de alumnos. Se trataba, según ha reconocido el propio B.B.B., de un proyecto personal objeto de un ponencia realizada para el I Congreso de Innovación en Orientación para la Universidad (CIES 2006), organizado por la UPV, en el que se inscribió igualmente a título personal.
En definitiva, no fue la entidad Conselleria D´Educació de la Generalitat Valenciana la que, contraviniendo la normativa de protección de datos de carácter personal, reveló los datos de los afectados a una entidad tercera, sino que fue B.B.B. el que los obtuvo de los ficheros de alumnos de la Consellería, a los que tenía acceso en virtud del cargo que ocupaba, es decir, como director del instituto en el que cursaba estudios la hija del denunciante, y los incluyó en el documento que posteriormente facilitó a la UPV. Por tanto, procede exonerar de responsabilidad a la Conselleria D´Educació de la Generalitat Valenciana y declarar que por la misma no se ha infringido el artículo 11.1 de la LOPD.
A este respecto, debe considerarse lo dispuesto en 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 (en lo sucesivo LRJPAC), según el cual *"... sólo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia".*
Por otra parte, no se formula imputación alguna por la posibles las responsabilidades que derivan de la conducta mantenida por B.B.B., por el presunto tratamiento de datos realizado por el mismo sin consentimiento de los afectados (infracción del artículo 6 de

la LOPD) y la presunta revelación de datos efectuada a la UPV (infracción del artículo 10 de la LOPD), tipificadas como infracciones grave y leve, respectivamente, en los artículos 44.3.d) y 44.2.e) antes citados, considerando que esta última ya había prescrito en el momento en que se formuló la denuncia y la infracción grave señalada prescribió inmediatamente después de formulada la misma y recibida en esta Agencia Española de Protección de Datos (02/10/2008), por el transcurso de más de dos años desde que el momento en el que pudo cometerse dicha infracción (19/10/2006), sin que esta Agencia hubiese dispuesto del tiempo necesario para desarrollar la oportuna investigación y la consiguiente apertura del procedimiento sancionador, de haber resultado esta procedente.
En relación con B.B.B., el denunciante ha manifestado que es responsable de infracción no prescrita por la utilización del "Programa GESDOR" en unas jornadas celebradas en el IES Tiranc lo Blanc en febrero de 2008. Sin embargo, la documentación aportada tiene que ver con la celebración de dichas jornadas pero no acredita la utilización de los datos personales de los afectados.
Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DECLARAR que la **UNIVERSIDAD POLITÉCNICA DE VALENCIA** ha infringido lo dispuesto en el artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de la citada Ley Orgánica.

SEGUNDO: ARCHIVAR el procedimiento de declaración de infracción de las Administraciones Públicas seguido contra la **CONSELLERIA D´EDUCACIÓ DE LA GENERALITAT VALENCIANA (I.E.S. MONSERRAT)**.

TERCERO: REQUERIR a la **UNIVERSIDAD POLITÉCNICA DE VALENCIA** para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 6 de la LOPD.
Las resoluciones que recaigan en relación con las medidas y actuaciones adoptadas, deberán ser comunicadas a esta Agencia Española de Protección de Datos, de acuerdo con el artículo 46.3 de la LOPD. La citada comunicación deberá realizarse en el plazo de un mes.

CUARTO: NOTIFICAR la presente resolución a la **UNIVERSIDAD POLITÉCNICA DE VALENCIA**, a la **CONSELLERIA D´EDUCACIÓ DE LA GENERALITAT VALENCIANA (I.E.S. MONSERRAT)** y a **D. A.A.A.**.

QUINTO: 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.

Procedimiento Nº AP/00075/2009

RESOLUCIÓN: R/00259/2010
En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00075/2009**, instruido de oficio por la Agencia Española de Protección de Datos al **Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana)**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 4 de noviembre de 2008 el Director de la Agencia Española de Protección de Datos acordó, a la vista de las informaciones aparecidas en diversos medios de comunicación, la iniciación de actuaciones previas de inspección al objeto de determinar si la instalación, en el Instituto de Enseñanza Secundaria Abastos de la ciudad de Valencia (en adelante IES Abastos), de un sistema de cámaras de videovigilancia y de un sistema de control de accesos con reconocimiento de huellas dactilares pudieran constituir hechos susceptibles de motivar la incoación de procedimiento sancionador por infracción a la normativa de protección de datos.

SEGUNDO: Con fecha 26 de noviembre de 2008 tuvo entrada en esta Agencia escrito procedente de la Delegación de Gobierno en la Comunidad Valenciana al que se adjuntaba la denuncia interpuesta por el "Sindicato de Estudiantes" (Confederación Estatal de Asociaciones de Estudiantes) en la que se solicitaba, por un lado, la apertura de expediente sancionador al Director del IES Abastos y, por otro lado, la depuración de las posibles responsabilidades de la Consejería de Educación de la Comunidad Valenciana con motivo de la instalación de los sistemas de seguridad y control de accesos anteriormente citados. Según el Sindicato de Estudiantes la instalación del referido sistema de videovigilancia, que permite la grabación de las imágenes captadas sin ningún control ni garantías legales, es una medida desproporcionada y arbitraria para la finalidad de seguridad con la que se justifica desde la dirección del Centro, haciendo especial hincapié en que la instalación de cámaras en los aseos de las chicas resulta discriminatoria y atenta a su derecho a la intimidad.

TERCERO: Con fecha 3 de diciembre de 2008 los servicios de Inspección de Datos de la AEPD realizaron una visita de inspección en el IES Abastos, en la que se encontraba presente el Director del mencionado Centro, quien realizó las siguientes manifestaciones:
- El instituto depende de la Consejería de Educación del Gobierno Autonómico de la Comunidad Valenciana, aunque tiene un Código de Identificación Fiscal independiente de ésta que se utiliza para facturar.
- La instalación de cámaras de vigilancia en sus dependencias pretendía evitar los actos vandálicos que venían produciéndose en distintas zonas del instituto.
- Dicha instalación, así como el sistema de control de acceso, fue aprobada en sesión ordinaria celebrada el día 9 de abril de 2008 del Consejo Escolar, conforme se comprueba en la copia del Acta de la sesión del Consejo Escolar ordinario celebrada dicho día, cuya copia fue aportada para su unión al Acta de Inspección. En el punto 4 del orden del día, relativo al" *Informe de dirección sobre el proyecto de videovigilancia y control de accesos para el centro y aprobación, si procede",* se hace constar que efectuadas las votaciones para la implantación del sistema de videovigilancia y de control de accesos la primera medida de las citadas se aprueba por unanimidad y la segunda por mayoría.

-El sistema de videovigilancia cuenta con 22 cámaras distribuidas en las tres plantas del recinto educativo. Se aporta un plano en el que aparecen señaladas las ubicaciones de las reseñadas cámaras de videovigilancia.
- Las imágenes son visualizadas únicamente en un monitor ubicado en el cuarto donde está instalado el sistema de control de las cámaras y al que tiene acceso el director del instituto o el jefe de estudios en su ausencia. Se graban en un dispositivo provisto de disco duro y se conservan aproximadamente durante 15 días, grabándose las imágenes nuevas sobre las antiguas.
- En el hall de entrada al instituto hay dos carteles informativos sobre la existencia de las videocámaras. Además, en la secretaría del instituto hay un modelo de información que se entrega a todas aquellas personas que lo solicitan.
- La empresa que ha instalado los sistemas de videovigilancia y de control de accesos se denomina VALBIT INGENIERIA, S.L. No se ha suscrito ningún contrato entre dicha empresa y el IES Abastos, no constando tampoco que la mencionada sociedad, que también se encarga del mantenimiento del sistema, se encuentre inscrita como empresa de seguridad en el Ministerio del Interior.
- No hay cámaras de videovigilancia que tomen imágenes de la vía pública.
- Las imágenes sólo se visualizan cuando algún alumno o persona lo solicita con motivo de algún robo o acto vandálico y la visualización se produce siempre en presencia del director o del jefe de estudios.
- Las cámaras de videovigilancia están activas las 24 horas del día y sólo graban cuando detectan movimiento.
- El fichero que se genera con las imágenes grabadas no ha sido inscrito en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos.
- El sistema de control de acceso no se ha llegado a poner en funcionamiento, por lo que no se han tomado las huellas digitales de ningún alumno o persona relacionada con las actividades desarrolladas por el instituto. El representante del Instituto señala respecto de este asunto que se está revisando la posibilidad de instalar algún sistema de control de acceso diferente del previsto a través de huella digital.

CUARTO: En la comprobación efectuada en el citado IES por los inspectores actuantes en los distintos lugares donde se encontraban ubicadas las cámaras y en la sala donde se emplazaba el monitor que permitía la visualización de las imágenes captadas se constato que:
- En el hall de entrada hay dos videocámaras enfocando a la entrada. Debajo de cada una de ellas hay un cartel informativo igual al que se publica en la Instrucción de videovigilancia 1/2006 de la Agencia Española de Protección de Datos.
- En la secretaría se encuentra la carpeta que contiene los formularios informativos a disposición de los interesados..
- El sistema de control de acceso no está en funcionamiento.
- Hay distintas cámaras en cada una de las dos alas de que consta el edificio con la siguiente ubicación, dos instaladas frente a la entrada a los baños de los profesores, cuatro cámaras cruzadas en los pasillos enfocando a las taquillas que utilizan los alumnos, dos controlando la puerta de acceso a los baños de chicas, y dos controlando la puerta de acceso a los baños de chicos.
- En la planta alta hay dos cámaras enfocando los pasillos, concretamente enfocando los pasillos y las puertas de entrada a los baños de chicos y chicas.
- Se comprueba que en total hay 22 cámaras instaladas en el instituto.- Respecto a las cámaras ubicadas en los baños, se comprueba y así lo manifiesta el director del instituto, que se instaló una cámara dentro del aseo de las chicas enfocando a la puerta de entrada. Esta cámara actualmente se ha cambiado de ubicación sacándola fuera del baño instalándola frente a la puerta de entrada al aseo de chicas.

- El local donde se encuentra instalado el dispositivo que controla las cámaras de vigilancia local está cerrado con llave ya que es el despacho donde se deposita material informático. El dispositivo se encuentra ubicado en otro local anexo también cerrado con llave.
- El sistema de videovigilancia tiene grabadas imágenes desde el 15 de octubre de 2008, comprobándose que las imágenes captadas permiten identificar a las personas.
- En la fecha en que se realiza la inspección, se pueden reproducir las imágenes grabadas en el baño de las chicas con la instalación de la cámara en el lugar inicial dentro del aseo.
- El acceso a las imágenes se encuentra protegido por usuario y contraseña.
- En los pasillos donde están las taquillas de los alumnos hay algunas rotas. Por otra parte, también se comprueba que algunos baños de los chicos están cerrados y aparece un cartel en la puerta que indica que están cerrados por actos vandálicos.

QUINTO: Con fecha 8 de octubre de 2009 se verificó que en el Registro General de la AEPD la Consejería de Educación de la Generalidad Valenciana no figura inscrita como responsable de ningún fichero de titularidad pública de Videovigilancia.

SEXTO: Con fecha 15 de octubre de 2009**,** el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas al Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana) por las presuntas infracciones a lo dispuesto en los artículos 4.1, 6.1 y 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas las dos primeras infracciones citadas como graves en el artículo 44.3.d) de dicha norma y también tipificada como grave la última de las infracciones citadas en el artículo 44.3.a) de dicha Ley. Dicho acuerdo de inicio fue notificado al IES Abastos, a la citada Consejería de Educación de la Generalidad Valenciana y al SE con fecha 23 de octubre de 2009.

SÉPTIMO: Con fecha 12 de noviembre de 2009 tiene entrada en esta Agencia escrito de alegaciones formulado por la Consejería de Educación de la Generalidad Valencia en el que, básicamente, se exponen las siguientes alegaciones al objeto de solicitar el archivo del procedimiento nº AP/00075/2009:
- En cuanto a la infracción al artículo 4.1 de la LOPD, en primer término se invoca el informe del Gabinete Jurídico de la Agencia de Protección de Datos nº 2006- 0262 que considera una medida proporcional y justificada la implantación de los sistemas de videovigilancia en los centros docentes cuando se cumplen los requisitos de idoneidad, para en segundo lugar reseñar que *"La instalación de videocámaras en el ÍES Abastos de la ciudad de Valencia tiene por objeto vigilar las distintas dependencias del centro escolar, por la obligación de defensa, protección y custodia del patrimonio de la administración pública y, también, por la atribución de responsabilidad a los centros educativos sobre los alumnos y sobre los actos de éstos mientras se encuentren bajo la vigilancia o control de profesorado."*
En apoyo de dicho argumento se citan el artículo 1903, párrafo 5º, del Código Civil, lo dispuesto en materia de responsabilidad patrimonial de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJAP) y los artículos 28 y 29 de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas. Se hace especial hincapié para justificar la idoneidad del sistema implantado en que la decisión de instalar el sistema de videovigilancia se adoptó por el Consejo Escolar del Instituto como *"órgano colegiado de gobierno en el que participan todos los sectores de la comunidad educativa: padres y madres o tutores legales de los alumnos, profesorado,*

alumnado (sector entre cuyos representantes no se encuentra el sindicato denunciante), personal de administración y servicios, que acordó, por unanimidad, la implantación del sistema de videovigilancia, habida cuenta de las situaciones que se habían generado en el centro (robos de material, actos vandálicos...), y como único mecanismo eficaz para garantizar la seguridad de las personas y de las instalaciones", de conformidad con lo previsto en "el Reglamento Orgánico y Funcional de los Institutos de Educación Secundaria, aprobado por Decreto del Consell 234/1997, de 2 de septiembre, en cuanto determina que "los órganos de gobierno [de los centros docentes] velarán por la protección de los derechos del alumnado así como por el cumplimiento de sus deberes." Asimismo, se pone de manifiesto que el Sindicato denunciante no sólo no tiene representación en el consejo escolar del centro sino que no concurrió al proceso electoral del sector alumnos. También, se propone la apertura de un período de práctica de prueba para aportar los documentos que acreditan la necesidad de adoptar medidas necesarias en orden a evitar las situaciones descritas.
- En cuanto a la infracción al artículo 6.1 de la LOPD se indica que no resulta necesario contar con el consentimiento de los afectados cuando la grabación se realiza por motivos de seguridad, , incluyendo a menores y a terceras personas ajenas al centro, toda vez que la empresa de seguridad que presta el servicio, "Seguretat i Autoprotecció Valenciana", cumple con los requisitos de la Ley 23/1992, de 30 de julio, de Seguridad Privada, causa por la que, de conformidad con el contenido del informe 0345/2009 del Gabinete Jurídico de la AEPD, está legitimado el uso del tratamiento de las imágenes "por la existencia de una norma con rango de Ley habilitante".
- En cuanto a la infracción del artículo 20 de la LOPD se reconoce que *"en la fecha de instalación del sistema de videovigilancia, no se había publicado en el boletín oficial correspondiente la disposición general de creación del fichero, aunque, a instancia del propio centro docente se han iniciado los trámites necesarios tendentes a corregir dicho extremo."*

OCTAVO: Con fecha 17 de noviembre de 2009 la Instructora del procedimiento solicitó a la Confederación Estatal de de Asociaciones de Estudiantes (Sindicato de Estudiantes), en lo sucesivo también CEAE-SE, determinada documentación e información a los efectos de poder valorar la condición de interesado aducida por dicho Sindicato en el escrito registrado de entrada en esta Agencia con fecha 11 de noviembre de 2009, y a fin de acreditar la representación otorgada por la Comisión Ejecutiva Estatal del citado Sindicato a D. B.B.B. para que éste se personarse en el procedimiento en nombre y representación del SE.
El mencionado escrito de autorización venía acompañado de escrito de personación y propuesta de prueba formulado por el nombrado representante del SE, al que se adjunta la impresión de una serie de artículos periodísticos relacionados con la instalación de cámaras de videovigilancia en el mencionado Instituto, y en el que se exponían, en síntesis, las siguientes alegaciones:
- Que el Sindicato se persona como parte interesada en el procedimiento n° AP/00075/2009, por la defensa de los derechos colectivos de los estudiantes, y, en particular, de los estudiantes directamente afectados del ÍES Abastos, entre los cuales hay afiliados al SE.
- Que la persona física del Director del IES Abastos, el Instituto como entidad propia y dependiente de la Consejería y la propia Consejería de Educación son responsables de la comisión de las siguientes infracciones graves a la LOPD:
* Infracción al artículo 4.1 de la LOPD por *"no adecuación y desproporción de la recogida y tratamiento de los datos de carácter personal" en relación con el artículo 12.4 de dicha norma por "uso y comunicación de los datos personales por el encargado de su recogida y tratamiento contrario a los principios de la LOPD; como por ejemplo sacar imágenes grabadas de dos chicas menores de edad dentro del*

baño, visionándolo persona diferente a la que manifiestan que acceden con exclusividad el Director y el Jefe de Estudios ante la inspección de la AEPD, y emitirlas en las noticias de las cadenas de tv más vistas a nivel estatal, sin el consentimiento expreso de las menores y sus padres o tutores"
* Infracción al artículo. 6.1 *"relativo al consentimiento inequívoco y expreso del afectado en concurrencia de su legal representante si se trata de menor de edad"*
*Infracción al artículo 20 por *"registro y archivo de datos personales en ficheros de titularidad pública sin respetar mínimamente ni los principios ni los procedimientos y garantías establecidos en la LOPD"*
Se hace hincapié en el incumplimiento de la Consejería de Educación de su obligación legal de asesorar, vigilar y garantizar el cumplimiento de la normativa legal vigente en los IES y de cubrir de aparente legalidad los incumplimientos de la LOPD.
- Que los hechos denunciados se cometieron de forma continuada durante meses, procediéndose por el Director del IES Abastos, sólo para evadir responsabilidades, a la subsanación del incumplimiento del deber de información ante las denuncias y medidas de presión de los propios estudiantes, padres y profesores del Instituto y en vistas de la inminente visita de Inspección de la AEPD.
Igualmente, en dicho escrito se solicita la adopción por la LOPD de la medida cautelar de retirada de todas las videocámaras y la destrucción controlada de toda la información obtenida por las mismas, por considerar que las medidas adoptadas para *"evitar actos vandálicos en las taquillas o los baños"* son desproporcionadas e ineficaces frente a la trascendencia real de las mismas, ya que se trata de conductas que se circunscriben al régimen de convivencia interno del ámbito educativo que pueden resolverse con otro tipo de medidas, tales como las campañas de concienciación y educativas y la colaboración de los conserjes y miembros de la comunidad educativa.
Asimismo se propone la práctica de una serie de medios de prueba tanto documental, como de imagen y sonido.

NOVENO: Con fecha 17 de noviembre de 2009, por parte de la instructora del procedimiento se inició el período de práctica de pruebas, dando por reproducidas, a efectos probatorios, el acuerdo de inicio de actuaciones previas de inspección, la denuncia interpuesta por el Sindicato de Estudiantes y su documentación adjunta, los documentos obtenidos y generados por los Servicios de Inspección, el Acta de Inspección E/1986/2008/I-01 y la documentación anexada a la misma, el Informe de actuaciones previas de Inspección del expediente E/01986/2008, las alegaciones al acuerdo de inicio presentadas por la Consejería de Educación de la Generalidad Valenciana y la incorporación, a los mismos efectos, de la documentación recabada en distintas páginas Web de Internet sobre una serie de informaciones aparecidas en distintos medios de comunicación relacionada con los hechos objeto de imputación.
Asimismo, en esa misma fecha se acordó solicitar a la mencionada Consejería la práctica de una serie de pruebas relacionadas con el sistema de videovigilancia instalado en el IES Abastos, así como aceptar la práctica de la prueba documental propuesta por ésta consistente en la aportación de una serie de documentos acreditativos de la necesidad de instalar videocámaras en el IES Abastos en orden a garantizar la seguridad de las personas y de las instalaciones.
Dicho acuerdo fue notificado tanto al IES Abastos como a la mencionada Consejería con fechas 30 de noviembre y 2 de diciembre de 2009, respectivamente

DÉCIMO: Con fecha 27 de noviembre de 2009 se registra de entrada escrito suscrito por X.X.X., en calidad de representante del SE, justificando, por un lado, los intereses legítimos concretos, individuales o colectivos ostentados que podían resultar afectados por la resolución que se adopte en el procedimiento de declaración de infracción de

administraciones públicas y aportando, por otro lado, copia de los Estatutos de la CEAE-SE, de documentación acreditativa de la capacidad de obrar ostentada por los firmantes del acuerdo de fecha 25/10/2009 y copia de la resolución adoptada el 06/07/1987 por el Ministerio de Educación y Ciencia en virtud de la cual se incluye a la CEAE-SE en el Censo de Federaciones y Confederaciones de Alumnos con el número 5.
Con fecha 2 de diciembre de 2009 tuvo entrada escrito formulado por el Sr. B.B.B. en el que especificaban los artículos de los Estatutos de la CEAE-SE que amparaban la defensa legal de los derechos individuales o colectivos de los estudiantes que fueran vulnerados, afiliados o no al Sindicato, y que justificaban la legitimación, en base a los artículos 31.1c) y 31.2 de la LRJAP, para ser parte interesada en el AP/00075/2009 al objeto de defender los intereses de sus afiliados, directamente afectados por los hechos denunciados, como los derechos del resto de estudiantes del centro vulnerados colectivamente a raíz de las medidas denunciadas.

UNDÉCIMO: A la vista de de los fines previstos en el artículo 2.d) de los Estatutos de la CEAS-SE y de las facultades de la Comisión Ejecutiva Estatal recogidas en los apartados c) y e) del artículo 14 de dichos Estatutos, junto con otra documentación que acreditaba capacidad de obrar de los firmantes del acuerdo de fecha 25/10/2009, se consideró que dicha Confederación había acreditado la ostentación de intereses legítimos colectivos, acordándose con fecha 3 de diciembre de 2009 considerar a la CEAS-SE como parte interesada en el procedimiento AP/00075/2009, de conformidad con lo previsto en el artículo 31.1c) de la LRJAP, y como personada en dicho procedimiento, siguiéndose las actuaciones del mismo con la persona nombrada por dicha Confederación.
Asimismo, con esa misma fecha de 3 de diciembre de 2009 se acordó, en el marco de trámite de práctica de pruebas, dar por reproducidas, a efectos probatorios, las alegaciones al acuerdo de inicio AP/00075/2009 presentadas por CEAS-SE, aceptar la práctica de prueba propuesta por CEAS-SE consistente en incorporar al procedimiento el dossier de prensa elaborado por el SE y solicitar a CEAS-SE la práctica de los siguientes medios de prueba:
- Prueba acreditativa de las manifestaciones efectuadas relativas a que el visionado de las imágenes se realizaba por persona diferente del Director o del Jefe de Estudios del IES Abastos, con especificación de la identidad de las personas que efectivamente lo realizaban.
- Indicación del período de tiempo en que se captaron y grabaron imágenes en los lavabos de las alumnas y acreditación de que no se cumplió por el mencionado Instituto el deber de información recogido en el artículo 3 de la Instrucción 1/2006, de 8 de noviembre, de la AEPD.
En cuanto a la práctica de prueba propuesta por CEAS-SE consistente en que la AEPD incorporase al procedimiento en soporte de imagen y sonido la grabación de los diferentes reportajes periodísticos que se emitieron en las principales cadenas de televisión estatales y autonómica, incluso requiriendo a las principales cadenas de televisión o medios de prensa escrita para que aporten sus archivos, se comunicó a la representación de dicho SE que se consideraba innecesaria, de conformidad con lo previsto en los artículos 80.3 y 137.4 de la LRJAP y el artículo 17.2 del Real Decreto 1398/1993, de 4 de agosto, que aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora, toda vez que ya se habían incorporado al procedimiento documentos que justificaban tanto la captación y grabación de imágenes de alumnas del citado Instituto en el aseo de chicas como la instalación de videocámaras en otras zonas del Instituto que permitían la captación de imágenes de las personas que se encontrasen en su ángulo de enfoque, tales como la documentación recabada por esta AEPD, el Acta de Inspección de fecha 03/12/2008

realizada en el IES Abastos, en la que además constaba que los inspectores actuantes comprobaron que el sistema tenía grabadas imágenes desde el día 15/10/2008 y *"que en esa fecha se pueden reproducir las imágenes grabadas en el baño de las chicas con la instalación de la cámara en el lugar inicial dentro del aseo"*, e incluso el propio dossier de prensa adjuntado por el SE a su escrito de alegaciones y personación.
Asimismo, también se comunicó a dicho representante la denegación por improcedente de la prueba consistente en que *"se requiera a la Consejería de Educación que especifique en qué otros centros de estudio públicos, concertados y privados dependientes de su competencia hay instalados medios similares de videovigilancia y recogida de huellas dactilares, y a partir de dicha información que esta AEPD inicie actuaciones preliminares de inspección y averiguación de si se están cometiendo más infracciones de la LOPD",* ya que dicha propuesta suponía plantear nuevas pretensiones fuera del objeto del presente procedimiento de declaración de infracción de administraciones públicas, el cual se inició después de la realización de las actuaciones de inspección acordadas de oficio por el Director de la AEPD con motivo de la instalación de cámaras y utilización de huellas dactilares para el control de accesos en el IES Abastos y después de la recepción de la denuncia formulada por los mismos hechos por el Sr. B.B.B., en representación del SE.
La práctica de las nuevas pruebas consta como notificada al IES Abastos y al representante del SE con fecha 9 de diciembre de 2009 y a la Consejería de Educación de la Generalidad Valenciana con fecha 17 de diciembre de 2009.

DUODÉCIMO: Con fecha 23 de diciembre de 2009 tiene entrada en esta Agencia escrito de la Consejería de Educación de la Generalidad Valenciana en el que como contestación a la práctica de pruebas que le fueron requeridas adjunta la siguiente documentación:
- Informe de la dirección del IES Abastos de Valencia sobre la necesidad de instalar un sistema de videovigilancia.
- Carpeta conteniendo contrato de renting BBVA, descripción de cámaras, plano de ubicación de las mismas y copia de contrato de prestación de servicios con "Seguretat i Autoprotecció Valenciana"
- Carpeta conteniendo copias de las Actas del Consejo Escolar del Centro de fechas 13 de febrero, 9 de abril y 6 de noviembre de 2008 y del comunicado de prensa del Instituto de fecha 6 de noviembre de 2008.
- Carpeta relativa al proceso de creación del fichero - Carpeta con extractos contables de los ejercicios 2007 y 2008 recogiendo los gastos ocasionados por las reparaciones subsiguientes a los actos de vandalismo.
En el primero de los documentos reseñados, el Director del IES Abastos justifica la necesidad de la instalación del sistema de videocontrol y de la ubicación de determinadas cámaras por la situación creada por los desperfectos causados en los bienes del Instituto por distintos agentes y causas. Dichos desperfectos fueron especialmente notables y costosos a lo largo de los cursos 2006/2007 y 2007/2008 en los cuartos de baño más alejados del control de los conserjes y el profesorado. El cierre de estos baños durante varias semanas generó quejas entre el alumnado y los representantes del sector de los padres en el Consejo Escolar del Centro, provocando también malestar entre el resto de los miembros de la comunidad educativa.
Por tal motivo se propuso al claustro de profesores y al Consejo Escolar del Centro la instalación de un sistema de videovigilancia con fines disuasorios y como medio para identificar a los autores de los daños, a la par que serviría de medida preventiva para frenar la desaparición de material informático del centro que se estaba produciendo. Dicha propuesta se aprobó por mayoría en el claustro y por unanimidad en el Consejo Escolar.

A continuación se cita que con fecha 15 de octubre de 2008 entró en funcionamiento el sistema de videovigilancia, indicándose que 4 de las 24 cámaras se instalaron en el interior de los baños de los alumnos durante 15 días, período en el que no hubo ningún incidente reseñable ni ninguna queja formal. Siendo a raíz de la denuncia ante la prensa efectuada el día 1 de noviembre por el SE, que no ostenta ninguna representación en el Centro, que como medida cautelar el día 3 de noviembre se detiene la grabación y el día 4 de noviembre se retiran dichas cámaras del interior de los baños, pasando a reubicarse dos de ellas en el exterior de los baños y a retirarse definitivamente las otras dos, produciéndose al día siguiente nuevos desperfectos en uno de los baños que tiene que volver a ser clausurado.
Asimismo se señala que después de la notificación del acuerdo de apertura de expediente se realizaron gestiones ante la Consejería de Educación a fin de instar el registro del fichero en la forma correspondiente.
DECIMOTERCERO: Con fecha 22 de enero de 2010, 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 declarase, en primer lugar, que el Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana) ha infringido lo dispuesto en los artículos 4.1 y 20 de la LOPD, lo que supone la comisión de sendas infracciones tipificadas como graves en los artículos 44.3.d) y 44.3.a), respectivamente, de la dicha norma, y, en segundo lugar, el archivo de las actuaciones seguidas al Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana) por supuesta infracción a lo dispuesto en el artículo 6.1 de la LOPD.
Igualmente se propuso que se requiriera al citado Instituto la adopción de las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de los artículos 4.1 y 20 de la mencionada Ley, así como la comunicación de la Resolución que se adopte al Defensor del Pueblo de conformidad con lo establecido en el artículo 46.4 de la Ley Orgánica 15/1999.
La mencionada propuesta de resolución figura como notificada al Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana) con fecha 25 de enero de 2010, a D. B.B.B., en representación del Sindicato de Estudiantes (CEAE-SE) con fecha 26 de enero de 2010, y a la Consejería de Educación de la Generalidad Valenciana, Dirección Territorial de Educación de Valencia, con fecha 8 de febrero de 2010.
No consta que se haya formulado escrito de alegaciones a dicho propuesta de resolución por ninguno de los destinatarios de la misma.

HECHOS PROBADOS

PRIMERO: La implantación de un sistema de videovigilancia en el IES Abastos fue aprobada en sesión ordinaria del Consejo Escolar celebrada el día 9 de abril de 2008, constando en el desarrollo del punto 4 del orden del día del Acta levantada con motivo de tal sesión, relativo al" *Informe de dirección sobre el proyecto de videovigilancia y control de accesos para el centro y aprobación, si procede",* que efectuadas las votaciones para la implantación del sistema de videovigilancia dicha medida se aprueba por unanimidad.

SEGUNDO: La instalación de cámaras de vigilancia en las dependencias del centro obedecía a razones de seguridad y vigilancia, ya que con tal medida se pretendía evitar los actos vandálicos y daños en bienes que venían produciéndose en distintas zonas del instituto, así como prevenir la desaparición de material informático que había ocurrido recientemente. (Folios 20 y 204)

TERCERO: No se ha acreditado que la empresa que instaló el sistema de videovigilancia, denominada VALBIT INGENIERIA, S.L. figure inscrita como empresa de seguridad en el correspondiente registro del Ministerio del Interior. (Folios 21 y 221)

CUARTO: En el momento de la entrada en funcionamiento del citado sistema, acaecido según el Director del citado Instituto con fecha 15 de octubre de 2008, había un total de 24 cámaras distribuidas por diferentes dependencias de las plantas del Instituto, cuatro de las cuales se ubicaban en el interior de cuatro baños utilizados por los alumnos. Posteriormente, con fecha 4 de noviembre de 2008, se procedió a retirar las cuatro cámaras reseñadas de los baños, reubicándose dos de ellas en la zona exterior de los mismos y dejándose de instalar las otras dos, de tal modo que a partir de esa fecha el sistema pasó a contar con 22 cámaras de videovigilancia, las cuales están activas las 24 horas del día y sólo graban cuando detectan movimiento.

QUINTO: En el desarrollo del punto 3 del Acta de la Sesión del Consejo Escolar Ordinario del mencionado Instituto, celebrada el día 6 de noviembre de 2008, titulado *"Informe de dirección sobre los siguientes apartados: Videocámaras y Próximas elecciones a CE"* consta que: *"Informa que, sensibilizados por esta problemática, hemos eliminado las cámaras de los cuartos de baño. Después de esta eliminación se han producido desperfectos en estos baños."* (Folios 245 al 250)

SEXTO: Con fecha 1 de abril de 2009 el IES Abastos suscribe contrato de prestación de servicios de seguridad con la empresa de seguridad SEGURITAT I AUTOPROTECCIÓ VALENCIANA. (Folios 227 al 233)

SÉPTIMO: Con fecha 3 de diciembre de 2008 los servicios de Inspección de Datos de la AEPD comprobaron en la inspección efectuada en el citado IES lo siguiente: (Folios 21 y 22)
- En el hall de entrada hay dos distintivos informativos de zona videovigilada y en la secretaría se encuentran los formularios informativos a disposición de los interesados.(Folio 33)
- El instituto cuenta con 22 cámaras instaladas. La ubicación de las mismas en cada una de las dos alas de que consta el edificio es la siguiente: dos instaladas frente a la entrada a los baños de los profesores, cuatro cámaras cruzadas en los pasillos enfocando a las taquillas que utilizan los alumnos, dos controlando la puerta de acceso a los baños de chicas, y dos controlando la puerta de acceso a los baños de chicos. En la planta alta hay dos cámaras enfocando los pasillos y las puertas de entrada a los baños de chicos y chicas. (Folio 22)
- Respecto a las cámaras ubicadas en los baños, se comprueba y así lo manifiesta el director del instituto, que se instaló una cámara dentro del aseo de las chicas enfocando a la puerta de entrada. Esta cámara actualmente se ha cambiado de ubicación sacándola fuera del baño instalándola frente a la puerta de entrada al aseo de chicas.
- El sistema de videovigilancia tiene grabadas imágenes desde el 15 de octubre de 2008, entre las que se encuentran las grabadas en el interior del baño de las chicas. Se comprueba que las imágenes almacenadas permiten identificar a las personas.
- El local donde se encuentra instalado el dispositivo que controla las cámaras de vigilancia está cerrado con llave. El dispositivo, a su vez, está ubicado en otro local anexo también cerrado con llave.
- El acceso a las imágenes se encuentra protegido por usuario y contraseña.

OCTAVO: Durante dicha actuación inspectora el director del mencionado Centro manifestó, entre otras afirmaciones, que: (Folios 21 y 205)

- Las imágenes son visualizadas en un monitor ubicado en el cuarto donde está instalado el sistema de control de las cámaras y al que tiene acceso el Director del instituto o el Jefe de Estudios, en su ausencia. Las imágenes capturadas se graban en un dispositivo provisto de disco duro, conservándose por un plazo aproximado de 15 días y grabándose las imágenes nuevas sobre las antiguas
- Las imágenes sólo se visualizan cuando algún alumno o persona lo solicita con motivo de algún robo o acto vandálico y la visualización se produce siempre en presencia del director o del jefe de estudios.

NOVENO: No consta que el fichero de videovigilancia de titularidad pública creado cuente con autorización de *disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente, y, por tanto, tampoco figura como* inscrito en el Registro General de Protección de Datos de la AEPD. (Folios 21, 43.bis (1,2,3), 93

FUNDAMENTOS DE DERECHO

I

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

II

Con carácter previo al análisis de los artículos de LOPD cuya vulneración se imputa al IES Abastos (Consejería de Educación de la Generalidad Valenciana) hay que señalar que dicha Ley Orgánica viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

El artículo 1 de la LOPD dispone que: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

El artículo 2.1 de la misma señala como ámbito de aplicación de la citada norma que: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado*"; definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como "*Cualquier información concerniente a personas físicas identificadas o identificable*s".

De acuerdo con lo anterior, resulta preciso determinar, en primer lugar, que ha de entenderse por dato de carácter personal. El artículo 3.a) de la LOPD considera dato de carácter personal "*cualquier información concerniente a personas físicas identificadas o identificables*".

Por su parte el artículo 5.1 del Reglamento de desarrollo de al LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, recoge en sus aparatados f) y o) las definiciones de *"datos de carácter personal"* y *"persona identificable".* Así, se considera *"datos de carácter personal*": *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables"* y *"persona identificable":* "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas*".

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable.
En el 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 personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, entiende por dato personal *"toda información sobre una persona física identificada o identificable; 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"*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.
El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas.
Para determinar si el supuesto que se analiza implica el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos.
En segundo lugar, debe analizarse el concepto de tratamiento de datos, este concepto se recoge en el artículo 3.c) de la LOPD, que define tratamiento de datos como aquellas "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones*, *consultas, interconexiones y transferencias*".
La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.
En el ámbito comunitario, la Directiva 95/46/CE en su Considerando 14 afirma: "(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;".
Así las cosas, la captación y grabación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal siempre que

dichas imágenes contengan *"cualquier información concerniente a personas físicas identificadas o identificables",* es decir, que permita o haga posible la identificación de las personas que aparecen en las mismas. En este supuesto, el sistema de videovigilancia instalado en el IES Abastos con fines de seguridad permite la captación, visualización en tiempo real de las zonas acotadas objeto de protección y de las personas afectadas por este tipo de tratamiento y grabación de dichas imágenes. Dicho tratamiento afecta, como mínimo, al personal docente y alumnado del centro, así como a terceras personas que se encuentren en el ángulo de enfoque de las zonas videovigiladas del Instituto. Es decir, ya que a efectos de la LOPD la imagen de una persona constituye un dato de carácter personal, nos encontramos ante un tratamiento que cae bajo la órbita de la normativa de protección de datos de carácter personal, toda vez que la información que captan las mencionadas cámaras contiene, entre otra información, datos concernientes a personas identificadas o identificables dado el entorno en el que se recogen y graban, y sobre las que suministran información relativa a la imagen personal de éstas, el lugar de su captación y la actividad o conducta desarrollada por los individuos a las que las imágenes se refieren.

III

Sentado lo anterior, procede resaltar que se encuentran sujetos al régimen sancionador establecido en la LOPD *"los responsables de los ficheros"* y *"los encargados de los tratamientos",* de acuerdo con lo dispuesto en el 43.1 de la citada norma. Ahora bien, la LOPD recoge y diferencia las figuras del responsable del fichero y del responsable del tratamiento.

Efectivamente, el artículo 3.d) de la LOPD, innovando respecto de la Ley Orgánica 5/1992, incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. Así conforme al citado artículo 3.d) el responsable del fichero o del tratamiento es *"la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*", considerándose en el artículo 5.1 q) del RDLOPD como tal a la "*persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados."* Por lo que debe entenderse que la expresión "responsables de los ficheros", contenida en el precitado artículo 43.1 de la LOPD, se refiere tanto a los responsables del fichero como a los responsables de los tratamientos.

El Tribunal Supremo, en su Sentencia de 26/01/2005, dictada en casación para unificación de doctrina, confirma la doctrina anteriormente expuesta al señalar que "*junto al responsable del fichero –que era en la Ley 5/1992- quien estaba sujeto al régimen sancionador establecido en dicha ley (art. 42) en la nueva Ley 15/1999 aparece un nuevo personaje, el responsable del tratamiento, como posible sujeto pasivo de la potestad sancionadora de la que hoy se llama –a partir de la Ley 62/2003, de 30 de diciembre- Agencia Española de Protección de Datos (artículo 43), Véase lo que dicen uno y otro precepto:*

Ley 5/1992 <<Art. 42. Responsables: 1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley>>. Ley 15/1999 << Art. 43. Responsables: 1- Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente ley>>. Y esto es así porque la nueva Ley Orgánica –a diferencia de la vieja Ley Orgánica, que atribuía la potestad de decidir sobre la finalidad, contenido y uso del tratamiento únicamente al responsable del fichero- reconoce que esa decisión pueda tomarla –y así ocurre muchas veces- el responsable del tratamiento.

He aquí el nuevo texto: Ley 15/1999. <<Artículo 3. A los efectos de la presente Ley se entenderá por: [...] d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento>>.

No se trata como se ve de un mero cambio de redacción, de un simple giro gramatical, o una innovación puramente estilística. Es algo más profundo: estamos ante un cambio esencial en el modo de afrontar la regulación de las relaciones que se entablan entre quienes manejan los datos y el titular de los mismos."

De lo expuesto se desprende que, en este supuesto, el IES Abastos es responsable del tratamiento de las imágenes que incluyan datos de carácter personal captados por las cámaras que integran el citado sistema de seguridad privada y del tratamiento derivado de su visualización y grabación, estando, por lo tanto, sujeto al régimen de responsabilidad recogido en el Título VII de la LOPD. Esta afirmación encuentra su justificación en que, con independencia de las características particulares del sistema instalado, el mencionado Instituto decidió la realización de un tratamiento de datos personales, ya que resolvió la instalación en distintos lugares del centro de un sistema

de cámaras que captaban las imágenes de las personas que se encontraban en el ángulo de visión de aquéllas, y estableció, igualmente, que la finalidad, contenido y uso del citado tratamiento sería la vigilancia y control con fines de seguridad.

IV

El apartado 1 del artículo 6 de la LOPD, cuya posible vulneración se imputa en el presente procedimiento sancionador al IES Abastos, y el apartado 2 del mismo precepto disponen que:
"*1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*
2. *No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.".*
El artículo 3 de la LOPD define en su apartado h), como consentimiento del interesado "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".*
El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "...*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)".*
Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.
Una vez sentado que la captación y grabación de imágenes con fines de vigilancia y control se encuentra plenamente sometida a lo dispuesto en la LOPD cuando la recogida y tratamiento de dichas imágenes,- que incluye su grabación, captación, transmisión, conservación, almacenamiento, visualización, reproducción o tratamiento resultante de los datos personales relacionados con las imágenes-, permita la identificación de las personas que aparecen en las mismas, debe tenerse en cuenta que el tratamiento de datos en materia de videovigilancia se regula de forma específica en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en cuyos artículo 1.1 y 2 se dispone :
"1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras. El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de

imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas. Se considerará identificable una persona cuando su identidad puede determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados. Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma."
"Artículo 2. 1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia."
En el presente procedimiento consta que el sistema de videovigilancia instalado en el aludido Instituto disponía de dispositivos que permitían la captación, transmisión, visualización y grabación de imágenes que incluían datos de carácter personal de quienes accedían a las zonas objeto de videovigilancia, por lo que, de conformidad con lo anteriormente expuesto, se ha producido desde su entrada en funcionamiento un tratamiento de datos de carácter personal al amparo de la Ley Orgánica 15/1999 y dentro del ámbito de aplicación de la reseñada Instrucción 1/2006, de 8 de noviembre, y, por lo tanto, sometido al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD.

V

En el presente caso, la legitimación del tratamiento de los datos de carácter personal en materia de videovigilancia procedería de la Ley 23/1992, de 30 de julio, de Seguridad Privada, (en adelante LSP), por afectar a espacios privados, siempre y cuando la prestación de los servicios de instalación y mantenimiento de sistemas de seguridad se realizara por una empresa de seguridad autorizada por el Ministerio del Interior. Así , el artículo 1.1 de la LSP regula "*la prestación por personas, físicas o jurídicas, privadas de servicio de vigilancia y seguridad de personas o de bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de seguridad pública*", añadiendo el artículo 1.2 de la misma norma que "*A los efectos de la presente Ley, únicamente pueden realizar actividades de seguridad privada y prestar servicios de esta naturaleza las empresas de seguridad y el personal de seguridad privada, que estará integrado por los vigilantes de seguridad, los jefes de seguridad y los escoltas privados que trabajen en aquéllas, los guardas particulares del campo y los detectives privados*".
El artículo 5.1 e) de la LSP en la redacción vigente en la fecha de los hechos, anterior a la entrada en vigor con fecha 27 de diciembre de 2009 de la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio, disponía que*: "Con sujeción a lo dispuesto en la presente Ley y en las normas reglamentarias que la desarrollan, las empresas de seguridad únicamente podrán prestar o desarrollar los siguientes servicios y actividades (…) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad"*. Esta previsión se reitera en el artículo 1 del Reglamento de Seguridad Privada, aprobado por Real Decreto 2364/1994, de 9 de diciembre (en adelante RSP).

De este modo, la Ley habilitaría que los sujetos previstos en su ámbito de aplicación puedan instalar dispositivos de seguridad, entre los que podrían encontrarse las cámaras, siempre con la finalidad descrita en el citado artículo 1.1 de la LSP.
Para la efectiva puesta en funcionamiento de la medida, el artículo 6.1 de la LSP dispone que: *"Los contratos de prestación de los distintos servicios de seguridad deberán en todo caso consignarse por escrito, con arreglo a modelo oficial, y comunicarse al Ministerio del Interior, con una antelación mínima de tres días a la iniciación de tales servicios".*
El artículo 20 del RSP regula el procedimiento de notificación del contrato, la autoridad competente y el régimen aplicable a la contratación del servicio por las Administraciones Públicas y a supuestos excepcionales que exijan la inmediata puesta en funcionamiento del servicio.
Por último, el artículo 7 de la LSP establece, entre otros requisitos, que para la prestación privada de servicios o actividades de seguridad las empresas de seguridad habrán de obtener la oportuna autorización administrativa mediante su inscripción en un Registro que se lleva en el Ministerio del Interior.
En consecuencia, siempre que se hubiera dado cumplimiento a los requisitos formales establecidos en los artículos precedentes (inscripción en el Registro de la empresa y comunicación del contrato al Ministerios del Interior), las empresas de seguridad autorizadas podían instalar dispositivos de seguridad en ámbitos privados, entre los que se encontrarían los que tratasen imágenes con fines de videovigilancia, existiendo así, en principio, en lo que se refiere a la normativa de protección de datos una habilitación legal para el tratamiento de los datos de carácter personal captados en espacios privados a través de cámaras con fines de videovigilancia.
Relacionando las señaladas normativas de protección de datos y de seguridad privada con los hechos que han resultado probados de las actuaciones practicadas en el procedimiento de declaración de infracción de administraciones públicas, se constata que el IES Abastos trató, entre el 15 de octubre de 2008 y el 1 de abril de 2009, datos de carácter personal de los afectados por el tratamiento de las cámaras de videovigilancia sin contar con el consentimiento inequívoco de los mismos y sin estar, tampoco, amparado por habilitación legal para ello, ya que el sistema de videovigilancia se instaló y estuvo en funcionamiento durante dicho período sin cumplir con los requisitos y exigencias de la LSP antes descritos, dado que VALVIT INGENIERÍA, S.L., empresa instaladora del circuito de cámaras en cuestión, no tenía la condición de empresa de seguridad.
En consecuencia, no puede estimarse el alegato relativo a que el tratamiento de las imágenes realizado no precisaba del consentimiento de los afectados por estar legitimado por la LSP, ya que el Instituto imputado no formalizó contrato de prestación de servicios de seguridad con la empresa SEGURITAT I AUTOPROTECCIÓ VALENCIANA, registrada como empresa de seguridad con el nº ****, hasta el 1 de abril de 2009, es decir, después de varios meses de estar tratando los datos de las personas cuya imagen se recogía por las cámaras de videovigilancia y, asimismo, con posterioridad a la actuación inspectora llevada a cabo por la AEPD en el Centro con fecha 3 de diciembre de 2008.
Este criterio no es contrario al contenido del informe 0345/2009 del Gabinete Jurídico de la AEPD citado por la Consejería de Educación de la Generalidad Valenciana, toda vez que en el mismo se indica que para que el tratamiento de las imágenes quedara legitimado, en base a la existencia de una norma con rango de Ley habilitante que eximiera del consentimiento de los afectados, se debía contratar con una empresa de seguridad que hubiera cumplido los requisitos exigidos por la LSP, circunstancia que en este supuesto no se produjo hasta después de varios meses iniciado el tratamiento.

VI

No obstante los razonamientos anteriores, los cuales prueban la comisión de la infracción imputada al artículo 6.1 de la LOPD por falta de habilitación legal para el mencionado tratamiento, ya que el mismo se produjo al margen de la LSP hasta la fecha en que se contrató con la empresa SEGURITAT I AUTOPROTECCIÓ VALENCIANA, debe analizarse la implicación que en supuestos como el que nos ocupa tiene la entrada en vigor de la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio, que tuvo lugar con fecha 27 de diciembre de 2009.

Hasta dicha fecha la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada. La mencionada Ley 25/2009 ha suprimido para la mayor parte de los casos estas exigencias, al liberalizar la comercialización, entrega, instalación y mantenimiento de estos dispositivos, de forma que ya no será necesario acudir para su puesta en funcionamiento a una empresa de seguridad privada ni cumplir las obligaciones de notificación del contrato al Ministerio del Interior.

En concreto, el artículo 14 de la nueva Ley modifica la letra e) del artículo 5.1 de la LSP, que queda redactada como sigue: *"e) Instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad, de conformidad con lo dispuesto en la Disposición adicional sexta",* y añade una Disposición Adicional Sexta a dicha norma cuya redacción es la siguiente:*"Exclusión de las empresas relacionadas con equipos técnicos de seguridad: Los prestadores de servicios y las filiales de empresas de seguridad que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidas de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5, sin perjuicio de otras legislaciones específicas que pudieran resultarles de aplicación."*

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada podrá, a partir de la entrada en vigor de la referida norma, vender, entregar, instalar y mantener equipos técnicos de seguridad sin necesidad de cumplir las exigencias previstas en la LSP para tales empresas. De este modo, dado que la Ley 25/2009 permite la instalación y mantenimiento de dichos equipos por empresas distintas a las de seguridad privada, se legitima a quienes adquieran estos dispositivos para tratar los datos personales derivados de la captación de las imágenes sin necesidad de acudir a empresas de seguridad privada, siendo dicho tratamiento conforme a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora, esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

Si bien en función de la normativa aplicable en el momento de los hechos el tratamiento de datos de carácter personal realizado por el centro imputado a través de las referidas cámaras de videovigilancia carecía de habilitación legal desde la perspectiva de la AEPD, pues dicha instalación no fue realizada por empresa de seguridad registrada como tal, debe también considerarse que el artículo 9.3 de la Constitución Española garantiza la irretroactividad de las disposiciones sancionadoras

no favorables y que el artículo 128.2 de la LRJAP establece que: *"Las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor".*

Por consiguiente, tal como se ha establecido en distintas sentencias del Tribunal Constitucional, en este caso resulta de aplicación la retroactividad de las disposiciones posteriores favorables al infractor.

En consecuencia, cabe aplicar dicha retroactividad en el presente procedimiento sancionador en lo que respecta a que no procede exigir al IES Abastos que dicha instalación de videovigilancia estuviera realizada por una empresa de seguridad, dado que la nueva norma ha liberalizado las funciones de instalación y mantenimiento de dispositivos de seguridad que con anterioridad únicamente podían realizar las empresas de seguridad habilitadas como tales.

Ahora bien, sin perjuicio de la aplicación del principio de retroactividad por los motivos expresados hay que recordar que el tratamiento de las imágenes a través de dichos dispositivos deberá cumplir los restantes requisitos exigibles en materia de protección de datos de Carácter Personal, recogidos en la LOPD y, en particular, en la mencionada Instrucción 1/2006 de la AEPD, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida, el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de los interesados de impresos informativos, la implantación de medidas de seguridad y observación del deber de secreto y la notificación previa de la creación de ficheros de videovigilancia a la Agencia Española de Protección de Datos cuando se produzca grabación de imágenes, tal y como se recoge en el artículo 2.2 de dicha Instrucción que establece que *"la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia."*

Por ello, el tratamiento de las imágenes con información personal obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD, que dispone lo siguiente:

"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

En relación con dicho precepto el artículo 3 de la referida Instrucción 1/2006 establece lo siguiente en cuanto al modo en que hay de facilitar la información en los casos de videovigilancia::

"Los responsables que cuenten con sistemas de video vigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:

a) Colocar, en las zonas video vigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y

b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999. El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción."

A través del Acta de Inspección, levantada por el día 3 de diciembre de 2008, quedó constancia de la existencia en el centro de dos distintivos informativos en el hall del mismo anunciando que se trataba de una zona video vigilada y de la disposición de impresos con la información que está obligado a suministrar a los afectados que así lo soliciten.

Aunque el CEAE-SE ha manifestado que con anterioridad al anuncio de la visita de inspección de la AEPD el Centro no se cumplía el deber de información del tipo de tratamiento que se realizaba, dicha afirmación no se ha visto avalada por ningún tipo de prueba que diera verosimilitud a la misma, causa por la que, al no existir ninguna prueba de cargo acreditativa de dicha alegación, resulta de aplicación respecto de dicha cuestión el principio de presunción de inocencia del artículo 24.2 de la Constitución y lo previsto en el artículo 137.1 de la LRJAP que establece que "Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.".

VII

El tratamiento de datos de carácter personal mediante cámaras de videovigilancia instaladas en los baños de los alumnos supone la comisión, por parte del citado IES Abastos (Consejería de Educación de la Generalidad Valenciana) de la infracción del artículo 4.1 de la LOPD, cuyo tenor literal señala que: *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"*

El artículo 4 de la LOPD, con la denominación *"Calidad de datos"* es el primer precepto del título II dedicado a los *"Principios de calidad de datos",* que derivan del derecho fundamental a la protección de datos.

La STC 254/1993, de 20 de julio, señaló que *"el derecho fundamental a la protección de datos persigue, en suma, garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino; o dicho de otro modo, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno; mientras que el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos (..)".*

Al objeto de preservar ese derecho fundamental, la LOPD establece una serie de principios generales en esta materia, que se regulan en los artículos 4 a 12 de la LOPD, entre los que se encuentran la calidad de datos, el derecho a la información, el consentimiento del afectado, la seguridad de los datos, el deber de secreto y el acceso a los datos por cuenta de terceros. Los principios generales de protección de datos constituyen el contenido esencial de protección de datos y configuran un sistema de tutela que garantiza una utilización racional y razonable de los datos personales. Por ello a través de la configuración de estos principios el legislador aspira a constituir un sistema preventivo de tutela de la persona frente al tratamiento de sus datos.

La reciente SAN, Sección 1ª, de 25 de julio de 2006 (rec. 210/2005) establece que *"dichos principios sirven para delimitar el marco en el que debe desenvolverse cualquier uso o cesión de datos de carácter personal y para integrar la definición de los tipos de infracción definidos en el artículo 44 de la LOPD, pues este aborda la tipificación de las distintas infracciones mediante una remisión a los principios definidos en la propia ley".*

El Grupo de protección de las personas, ya citado, en lo que respecta al tratamiento de datos personales, en su Dictamen 4/2004, mencionaba en cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso.

En el apartado 1 del artículo 4 de la LOPD comienza sentado que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, de acuerdo con una serie de criterios, que se resumen en el principio de proporcionalidad.

Este artículo 4.1 de la LOPD consagra el "*principio de pertinencia en el tratamiento de los datos de carácter personal*", que impide el tratamiento de aquellos que no sean necesarios o proporcionados a la finalidad que justifica el tratamiento, debiendo restringirse el tratamiento de los datos excesivos o bien procederse a la supresión de los mismos. En consecuencia, el tratamiento del dato ha de ser pertinente y no excesivo en relación con el fin perseguido. Únicamente pueden ser sometidos a tratamiento aquellos datos que sean estrictamente necesarios para la finalidad perseguida. Por otra parte, el cumplimiento del principio de proporcionalidad no sólo debe producirse en el ámbito de la recogida de los datos, sino asimismo de respetarse en el posterior tratamiento que se realice de los mismos. Este criterio, se encuentra recogido también en el artículo 6 de la Directiva 95/46/CE, aparece también reflejado en el Convenio 108, cuyo artículo 5 c) indica que *"los datos de carácter personal que sean objeto de un tratamiento automatizado (...) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado".*

El mencionado precepto debe ponerse en correlación con lo previsto en el apartado 2 del citado artículo 4, según el cual: "*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.".* Las finalidades a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley.

Así, el uso de las instalaciones de cámaras y videocámaras debe seguir ciertas reglas que rigen todo el proceso desde su captación, transmisión, almacenamiento, reproducción hasta su cancelación. El IES Abastos debió tener en cuenta que debía existir una relación de proporcionalidad entre la finalidad de seguridad y vigilancia perseguida y el modo en el que se trataban los datos, garantizándose por los apartados 1 y 2 del mencionado artículo 4 de la LOPD el cumplimiento del principio de proporcionalidad y finalidad en todo tratamiento de datos personales.

Por ello, en relación con la instalación de sistemas de videocámaras, será necesario, como recoge el preámbulo de la Instrucción 1/2006 *"ponderar los bienes jurídicos protegidos".* Precisamente la redacción del artículo 4 de la mencionada Instrucción, relativo a los *"Principios de calidad, proporcionalidad y finalidad del tratamiento"*, establece:

"1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las

finalidades determinadas, legítimas y explicitas, que hayan justificado la instalación de las cámaras o videocámaras.
2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.
3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida".
Igualmente hay que valorar, tal y como se indica en la Instrucción 1/2006, de 8 de noviembre, que *"En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusitos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.*
En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.
En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.
En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones <<si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".

VIII

A la vista de la normativa anterior, el IES Abastos (Consejería de Educación de la Comunidad Valenciana) vulneró el artículo 4.1 de la LOPD y el artículo 4 de la citada Instrucción 1/2006, de 8 de noviembre, cuando decidió la instalación de cámaras de videovigilancia en el interior de cuatro baños utilizados por los alumnos del centro como un medio disuasorio para evitar actos vandálicos.
Según el mencionado Instituto el tratamiento de las imágenes que contenían datos de carácter personal obtenidos a través estas cuatro cámaras se llevó a cabo entre el 15 de octubre y el 4 de noviembre de 2009, fecha esta última en la que se retiraron las citadas cámaras de los baños reseñados y se procedió a la reubicación de dos de ellas fuera de los baños y a la retirada definitiva de las otras dos cámaras, pudiéndose constatar por los inspectores de datos de la AEPD que en el citado Instituto se conservaban imágenes grabadas desde el 15 de octubre de 2008 por las mencionadas

cámaras, cuya visualización permitía identificar a las personas captadas por las mismas.
El tratamiento de datos de carácter personal efectuado en ese período de tiempo mediante la utilización de las reseñadas cuatro cámaras se considera excesivo, no pertinente e inadecuado en relación con la finalidad de seguridad para la que se recogían las imágenes. Así, en razón de la privacidad de los espacios en que se capturaban dichas imágenes el Instituto debió ponderar, frente a la finalidad de seguridad y vigilancia que motivó su instalación, los derechos a la intimidad, a la propia imagen y a la protección de datos de las personas que se verían afectados por tal utilización de las cámaras, de forma que se cumpliera estrictamente el principio de proporcionalidad.
Es decir, aunque pueda resultar justificable el uso de técnicas de videovigilancia por motivos de seguridad, en ningún caso resulta admisible la instalación de cámaras en baños por la naturaleza de los derechos fundamentales que pueden verse afectados, entre los que se encuentra el de la protección de datos, debiendo tenerse en cuenta tal circunstancia a fin de respetar tales derechos y no captar imágenes de personas identificadas o identificables en dichos lugares, tal y como se ha comprobado ocurrió en los cuatro baños en que se usaron dispositivos de videovigilancia. Por lo tanto, se trataba de un tratamiento particularmente invasivo e intrusivo para la intimidad de las personas titulares de los datos tratados y para el derecho de disposición de los propios datos de los afectados, ya que la medida utilizada, aunque fuera susceptible de cumplir el objetivo de prevención frente a actos vandálicos en los bienes del centro, no era ponderada ni equilibrada por derivarse de ella perjuicios sobre los derechos de terceros en conflicto.
A mayor abundamiento dicho tratamiento se produjo en un entorno escolar que, si bien no se encuentra vedado a las prácticas de videovigilancia, si requiere la adopción de ciertas cautelas. De tal modo que la instalación de cámaras de videovigilancia en dichos ámbitos, con el fin de controlar conductas que puedan afectar a la seguridad ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia. Es por ello que el responsable del tratamiento debe analizar la proporcionalidad de la medida de instalar cámaras de videovigilancia en entornos sensibles, como son los baños, en atención a que en los mismos se producen manifestaciones de vida privada y dado que cuando la videovigilancia se circunscribe a ámbitos escolares puede afectar a menores de edad.
En consecuencia, el tratamiento del dato ha de ser pertinente y no excesivo en relación con el fin perseguido el IES Abastos no debió instalar cámaras de videovigilancia en cuatro baños del centro porque el tratamiento de los datos personales obtenidos a partir de las mismas resultaba excesivo y no pertinente al fin de seguridad perseguido con dicha medida.
La Consejería de Educación aduce que no se ha vulnerado el principio de proporcionalidad dado que la instalación de videocámaras en dichos baños estaba relacionada con los daños y desperfectos que se venían produciendo en los mismos desde el año 2005, además de para vigilar las distintas dependencias del centro escolar por la obligación de defensa, protección y custodia del patrimonio de la administración pública, y para responder, también, a la atribución de responsabilidad de los centros educativos sobre los alumnos y sobre los actos de éstos mientras se encuentren bajo la vigilancia o control del profesorado.
Frente a dicho alegato debe señalarse que la falta de proporcionalidad en el tratamiento de los datos de carácter personal se refiere, únicamente, al derivado de la instalación y utilización en el período reseñado de las cuatro cámaras ubicadas en el interior de los baños de los alumnos, habiéndose ya indicado con anterioridad los argumentos por los que tal tratamiento no se consideraba pertinente, sin que el hecho

de que tal medida se acordara por un órgano de gobierno colegiado del Instituto, como es el Consejo Escolar del centro, en el que participan los padres y madres o tutores legales de los alumnos, profesorado, alumnado, personal de administración y servicios y ayuntamientos en la gestión del instituto, suponga incidencia alguna en la irregularidad que ha supuesto dicho tratamiento.

Por lo tanto, se entiende, desde la perspectiva de la protección de datos, que la implantación de cámaras en el resto de lugares del Instituto se ajustaba al principio de proporcionalidad, cumpliendo, a los efectos de dicha garantía, los requisitos que se citan en el informe del Gabinete Jurídico de la AEPD 2006-0262 citado por la Consejería de Educación en sus alegaciones, afirmación que se realiza independientemente tanto de que la instalación no cumpliera hasta el 1 de abril de 2009 con los requisitos establecidos por la LSP vigente en esas fechas, y, por consiguiente, se tratase de un tratamiento que no contaba con habilitación legal que amparase el mismo sin el consentimiento inequívoco de los afectados, como sin perjuicio de la vulneración de otras obligaciones contenidas en la normativa de protección de datos.

En conclusión, la conducta analizada ha dado lugar a la vulneración por el IES Abastos de lo previsto en el aludido artículo 4.1 de la LOPD.

IX

La proporcionalidad es un elemento fundamental en todos los ámbitos en los que se instalen sistemas de videovigilancia, dado que son números os los supuestos en los que la vulneración del mencionado principio puede llegar a generar situaciones abusivas, por todo ello se trata de evitar la vigilancia omnipresente, con el fin de impedir la vulnerabilidad de las personas.

En este sentido, el Dictamen 4/2004, apartados D) y E), del Grupo del artículo 29 de la Directiva 95/46/CE, relativo al tratamiento de datos personales mediante vigilancia por videocámara, adoptado el 11 de febrero de 2004, señala lo siguiente :

"D) Proporcionalidad del recurso a la vigilancia por videocámara. El principio según el cual los datos deberán ser adecuados y proporcionales al fin perseguido significa, en primer lugar, que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas.

Dicho principio de proporcionalidadsupone que se pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, sistemas mejores y más potentes de alumbrado nocturno en las calles, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente.

El mismo principio también es aplicable a la selección de la tecnología adecuada, los criterios de utilización del equipo en concreto y la especificación de disposiciones para el tratamiento de datos en relación también con las normas de acceso y el período de retención. Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos). Dicho de otro modo, es necesario aplicar, caso por caso, el principio de idoneidad con respecto a los fines perseguidos, lo que implica una especie de obligación de minimización de los datos por parte del responsable del tratamiento. Si bien un sistema proporcionado de vigilancia por videocámara y alerta puede considerarse lícito cuando se producen varios episodios de violencia en una zona próxima a un estadio o se cometen agresiones repetidas a bordo de autobuses en zonas periféricas o cerca de las paradas de autobús, no ocurre lo mismo cuando se trata de un sistema destinado a evitar que se insulte a los conductores de autobús o que se ensucien los vehículos (tal y como le ha sido descrito a una autoridad de protección de datos), a identificar a ciudadanos responsables de infracciones de menor importancia, como dejar las bolsas de basura fuera del cubo o en zonas en las que está prohibido tirar basura, o a detectar a personas responsables de robos ocasionales en piscinas cubiertas. La proporcionalidad deberá evaluarse basándose en criterios más estrictos en lo que se refiere a lugares cerrados al público. El intercambio de información y experiencias entre las autoridades competentes de los diferentes Estados miembros puede ser útil en este sentido. Las consideraciones anteriores se refieren, en concreto, al uso cada vez más frecuente de vigilancia por videocámara con fines de autodefensa y protección de la propiedad (sobre todo, cerca de edificios públicos y oficinas, incluidas las áreas circundantes). Para este tipo de utilización se requiere la evaluación, desde un punto de vista más general, de los efectos indirectos derivados del recurso masivo a la vigilancia por videocámara (es decir, si la instalación de varios dispositivos es realmente un factor disuasorio o si los infractores o vándalos pueden, simplemente, desplazarse a otras zonas y actividades).

E) Proporcionalidad en la realización de actividades de vigilancia por videocámara

El principio según el cual los datos deben ser adecuados, pertinentes y no excesivos implica la evaluación minuciosa de la proporcionalidad de las medidas relativas al tratamiento de datos, una vez que la legalidad del mismo haya quedado validada. Las medidas para la grabación se establecerán teniendo en cuenta, en primer lugar, los siguientes aspectos: a) El ángulo visual con arreglo a los fines perseguidos (por ejemplo, si la vigilancia se realiza en un lugar público, el ángulo deberá establecerse de manera que no permita visualizar detalles o rasgos físicos que resulten irrelevantes para los fines perseguidos, o zonas situadas en el interior de lugares privados cercanos, en particular, si se utiliza el zoom). b) El tipo de equipo que se utilizará para filmar, es decir, fijo o móvil. c) Medidas reales de instalación, es decir, situación de las cámaras, utilización de plano fijo o cámaras móviles, etc. d) Posibilidad de aumentar las imágenes o realizar primeros planos, durante la grabación o después, es decir, una vez que se han almacenado las imágenes, y posibilidad de desenfocar o borrar imágenes individuales. e) Congelación de imágenes. f) Conexión con un «centro» para enviar señales de alarma sonoras o visuales. g) Medidas que se toman como resultado de la vigilancia por videocámara, es decir, cierre de entradas, convocatoria del personal de vigilancia, etc. En segundo lugar, deberá tenerse en cuenta la decisión que se va a tomar en cuanto a la retención de las imágenes y el plazo (éste último deberá ser bastante breve y estar en consonancia con las características específicas de cada caso). Si bien en algunos casos un sistema que sólo permita la visualización de imágenes en circuito cerrado, sin necesidad de grabar, puede ser suficiente (por ejemplo, en el caso de las cajas de un supermercado), en otros (por ejemplo, para proteger lugares privados), puede que esté justificado grabar imágenes durante unas cuantas horas y borrarlas automáticamente, sin exceder nunca el final del día o, como mucho, el final de la semana. Obviamente, esta regla tiene excepciones, como cuando se emite una señal de alarma o se realiza una petición que merece especial atención; en esos casos, hay motivos suficientes para esperar, durante un período breve, una posible decisión por parte de las autoridades policiales o judiciales. Por poner otro ejemplo, un sistema cuyo objetivo es detectar el acceso no autorizado de vehículos a centros urbanos y zonas de tráfico restringido, sólo deberá grabar imágenes en caso de que se cometa una infracción. La cuestión de la proporcionalidad también deberá tenerse en cuenta debidamente siempre que se considere que son necesarios períodos de retención más breves, que no deberán superar una semana (por ejemplo, imágenes de vigilancia por videocámara que puedan utilizarse para identificar a las personas que frecuentan un banco antes de que se cometa un robo). En tercer lugar, deberá prestarse atención a los casos en los que se facilita la identificación de una persona mediante la asociación de imágenes del rostro de dicha persona con otra información relativa a conductas actividades reproducidas (por ejemplo, en caso de asociación de imágenes y actividades realizadas por los clientes de un banco en un momento fácilmente identificable). En este sentido, deberá tenerse en cuenta la clara diferencia que existe entre la retención temporal de imágenes de vigilancia por videocámara captadas con un equipo situado a la entrada de un banco y la creación de bancos de datos que incluyan fotos y huellas dactilares facilitadas por los clientes del banco con su consentimiento, lo que supone una intrusión en mayor medida. Por último, deberá prestarse atención a las decisiones que se tomen con respecto tanto a la posible comunicación de los datos a terceras partes (lo que, en principio, no deberá implicar a entidades que no estén relacionadas con las actividades de vigilancia por videocámara) como a su posible revelación, total o parcial, en el extranjero o, incluso, en la red (también a la luz de las disposiciones relativas a la protección adecuada; véase el artículo 25 y siguientes de la Directiva). Obviamente, el requisito según el cual las imágenes deberán ser pertinentes y no excesivas, también se refiere a la combinación de información procedente de diferentes responsables del tratamiento de sistemas de vigilancia por videocámara. Las garantías mencionadas más arriba

pretenden implantar, también de manera operacional, el principio al que se hace referencia en la normativa nacional de varios países: el principio de moderación en el uso de datos personales (cuyo objetivo consiste en evitar o reducir al mínimo posible el tratamiento de datos personales). Este principio debería aplicarse en todos los sectores, teniendo en cuenta, también, el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales, o utilizando datos realmente anónimos, a pesar de que, inicialmente, pueda parecer necesario utilizar información personal. Las consideraciones anteriores también son aplicables cuando se da la necesidad justificada de racionalizar los recursos comerciales o de mejorar los servicios prestados a los usuarios" .

X

El artículo 44.3.d) de la LOPD tipifica como infracción grave: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave".*

En relación al tipo de infracción establecido en el citado artículo 44.3.d), la Audiencia Nacional, en Sentencia de 27/10/2004, ha declarado*: "Sucede así que, como ya dijimos en la Sentencia de 8 de octubre de 2003 (recurso 1.821/01) el mencionado artículo 44.3 d) de la Ley Orgánica 15/1999, aún no siendo, ciertamente, un modelo a seguir en lo que se refiere a claridad y precisión a la hora de tipificar una conducta infractora, no alberga una formulación genérica y carente de contenido como afirma la demandante. La definición de la conducta típica mediante la expresión "tratar los datos de carácter personal .." no puede ser tachada de falta de contenido pues nos remite directamente a cualquiera de las concretas actividades que el artículo 3.d) de la propia Ley incluye en la definición de "tratamiento de datos" (recogida, grabación, conservación, elaboración, ... de datos de carácter personal). Y tampoco cabe tachar de excesivamente genérico o impreciso el inciso relativo a que el tratamiento o uso de los datos se realice "... con conculcación de los principios y garantías establecidos en la presente Ley...", pues tales principios y garantías debidamente acotados en el Título II del propio texto legal bajo las rúbricas de Principios de la Protección de Datos (artículos 4 a 12) y Derechos de las Personas (artículos 13 a 19)".*

En el presente caso, la descripción de conductas que establece el artículo 44.3.d) de la LOPD cumple las exigencias derivadas del principio de tipicidad, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. El tipo aplicable considera infracción grave *"tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley",* por tanto, se está describiendo una conducta - el tratamiento de datos personales o su uso posterior – que precisa, para configurar el tipo, que la misma suponga vulneración de los principios y garantías establecidos por la LOPD.

En este supuesto el IES Abastos, en su condición de responsable del tratamiento, ha vulnerado el principio de calidad de los datos, en lo que se refiere al uso proporcional de los mismos en relación con el tratamiento de datos efectuado a partir de la captación y grabación de imágenes de alumnos en los baños del mencionado centro mediante cuatro cámaras de videovigilancia, el cual es un principio básico del derecho fundamental a la protección de datos, recogido en el artículo 4.1 de la LOPD y en el artículo 4. 1 y 2 de la Instrucción 1/2006, de 8 de noviembre.

Conviene recordar que desde el punto de vista material, la culpabilidad consiste en al capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico.

De conformidad el análisis realizado se ha incurrido en la infracción grave descrita. Así, ha quedado acreditado que en el período de tiempo comprendido entre el 15 de octubre y el 4 de noviembre de 2008 el mencionado Instituto utilizó cuatro cámaras de videovigilancia que captaban y permitían la grabación de imágenes de los alumnos de forma inadecuada y excesiva para el cumplimiento de los servicios de vigilancia y seguridad que originaron su instalación, actuación que no responde a la intervención mínima que exige la ponderación entre la finalidad de vigilancia y control de bienes y personas y la posible afectación por la utilización de las mencionadas videocámaras al derecho al honor, a la propia imagen, a la intimidad de las personas y a la normativa de protección de datos, constituyendo tal conducta infracción al reseñado artículo 44.3.d) de la LOPD .

XI

En cuanto a la imputación de la comisión de una infracción del artículo 20 de la LOPD dicho precepto señala que:
"*1. La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.*
2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos de carácter personal. d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo. e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros. f) Los órganos de las Administraciones responsables del fichero. g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción"
Asimismo, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, dispone en su artículo 7.1 en relación con la "Notificación de ficheros" lo siguiente:
"1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma. Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. "
En el caso analizado ha quedado acreditado que el IES Abastos recaba datos de carácter personal a través del sistema de cámaras de videovigilancia que está en funcionamiento en el Centro desde el 15 de octubre de 2008, procediendo a la grabación de las imágenes capturadas por dichas cámaras en un fichero de videovigilancia, todo ello sin mediar creación de fichero de titularidad pública mediante disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente y sin que dicho fichero, por lo tanto, hubiera sido notificado a la AEPD para su inscripción en el Registro General de Protección de Datos.

XII

El artículo 44.3.a) de la LOPD tipifica de infracción grave: "*Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente*".
En este supuesto, a través de las propias alegaciones formuladas por la Consejería de Educación de la Generalidad Valenciana, ha quedado acreditado que el IES Abastos inició la recogida de datos de carácter personal en un fichero de videovigilancia con anterioridad a su creación como fichero de titularidad pública en la forma prevista en el artículo 20 de la LOPD y sin estar inscrito en el Registro General de Protección de Datos, habiéndose procedido por dicho Instituto a solicitar, con fecha 4 de noviembre de 2009, la realización de los trámites necesarios para la regularización de tal situación ante dicha Consejería de Educación.
En consecuencia, dicha conducta supone incurrir en la infracción del artículo 20 de la LOPD, la cual encuentra su tipificación en el precepto trascrito.
Vistos los preceptos citados y demás de general aplicación, El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DECLARAR que el **Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana)** ha infringido lo dispuesto en los artículos 4.1 y 20 de la LOPD, tipificadas como infracciones graves en los artículos 44.3.d) y 44.3.a), respectivamente, de la dicha norma.

SEGUNDO: **DECLARAR** el archivo de las actuaciones seguidas al **Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana)** en el procedimiento de Declaración de Infracción de Administraciones Públicas AP/00075/2009, por supuesta infracción a lo dispuesto en el artículo 6.1 de la LOPD.

TERCERO: REQUERIR al **Instituto de Enseñanza Secundaria Abastos (Consejería de Educación de la Generalidad Valenciana)** para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de los artículos 4.1 y 20 de la LOPD.
Las resoluciones que recaigan en relación con las medidas y actuaciones adoptadas, deberán ser comunicadas a esta Agencia Española de Protección de Datos, de acuerdo con el artículo 46.3 de la LOPD. La citada comunicación deberá realizarse en el plazo de un mes.

CUARTO: Notificar la Resolución que se adopte al **Instituto de Enseñanza Secundaria Abastos, a la Consejería de Educación de la Generalidad Valenciana,** y a **D. B.B.B., en representación del Sindicato de Estudiantes (CEAE-SE).**

QUINTO: 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 Contenciosoadministrativo 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.

Procedimiento Nº AP/00081/2008

RESOLUCIÓN: R/01375/2009

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00081/2008**, instruido por la Agencia Española de Protección de Datos a la **UNIVERSIDAD DE ZARAGOZA**, vista la denuncia presentada por **D. X.X.X.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 3/3/2008 tiene entrada en esta Agencia un escrito de D. X.X.X. en el que denuncia a la Universidad de Zaragoza. En su escrito pone de manifiesto los siguientes hechos:

PRIMERO: Que el día 21 de Febrero de 2008 tuve conocimiento a través de la página web www...Z... de una información de un usuario en la que explicaba la falta de seguridad de la Universidad de Zaragoza en la protección de los datos de los estudiantes.

SEGUNDO: En esta información, se señala que a través de la página web http://...Y...../...../..... se pueden obtener las fotografías de los expedientes de aquellas personas relacionadas con la Universidad de Zaragoza.

TERCERO: Tras escribir mi NIP (identificador único de la Universidad de Zaragoza) en la página web http://...Y...../...../..... ha aparecido mi fotografía. Esta fotografía es la misma que aporte en su día al matricularme a la Universidad de Zaragoza.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información a la Universidad de Zaragoza, teniendo conocimiento de los siguientes hechos:

<< a) - La página web a la que se hace referencia en el escrito de la Agencia de Protección de Datos (http://...Y...../...../.....) no pertenece al dominio de direcciones de la Universidad de Zaragoza, pertenece a la empresa LYCOS España Internet Services S.L.

Que no ha habido ninguna cesión de datos a dicha empresa.

Que conocido el incidente al que se hace referencia en el escrito de la Agencia de Protección de Datos, y que más adelante se detallará, se procedió de inmediato a solucionar el problema quedando resuelto en apenas 60 minutos.

Ni por el mecanismo utilizado para visualizar la fotografía en el incidente que se analiza ni por ningún otro del que se tenga constancia se pudo (ni se puede) acceder a otros datos personales sin previa identificación y autenticación.

Se tomaron las medidas necesarias para que no pueda volver a suceder una situación similar a la que posibilitó el incidente que se trata.

b) La Universidad de Zaragoza al realizar la matrícula en cualquiera de sus Centros solicita a todos sus estudiantes una fotografía que se incorpora al expediente del alumno y se utiliza tanto para su gestión docente como para su participación en las actividades y servicios de la universidad. Dicho documento gráfico tiene como finalidad el poder relacionar a la persona que solicita cualquier servicio de la Universidad, con los datos que dicha persona presenta.

La utilización de dichos documentos gráficos a través de páginas web es un procedimiento normalizado en algunos programas comunes en las Universidades que utilizan esas aplicaciones como son, en la Universidad de Zaragoza:

- *WebCT, programa comercial específico para la enseñanza virtual (e-leaming).*
- *Milenium, programa de gestión de bibliotecas.*
- *Sigma, programa dedicado a la gestión académica.*

c) El día 22 de febrero de 2008 se tuvo conocimiento de la existencia de la página web de Lycos (http://...Y...../...../.....). En ella introduciendo 6 dígitos se obtenía, en algunas ocasiones, la fotografía de una persona; única y exclusivamente la imagen sin ningún otro dato que pudiese identificarla y/o posibilitar su puesta en relación con otros datos de carácter personal.
Se visualizaba una fotografía cuando el número introducido coincidía con lo que en la Universidad de Zaragoza se denomina NIP (número de identificación personal, asignado seriadamente a los alumnos de la universidad al matricularse). Se visualizaba la fotografía del estudiante cuyo NIP coincidía con esos dígitos.
Contrastada esta situación el día citado, a los 60 minutos de tener constancia del acceso indebido a las fotografías se suprimió el servicio y dejaron de visualizarse en Lycos las fotografías.
d) El origen del incidente se sitúa en las aplicaciones informáticas antes citadas: WebCT (aplicación para la enseñanza virtual) y Milenium (gestión de fondos bibliotecarios).
En la aplicación de gestión académica Sigma (tercera aplicación citada antes que utiliza las fotografías) se pudo utilizar una técnica diferente para la visualización de las fotografías que impedía el problema.
En ambas aplicaciones se accede a información personal previa identificación y autenticación de cada uno de los usuarios. Y a cada usuario se le muestra sólo la información pertinente: en WebCT (enseñanza virtual) a los profesores se muestra la 3/11
ficha de sus estudiantes y a cada estudiante a su propia ficha; en Milenium se muestra a los gestores de las bibliotecas la información pertinente de los usuarios de las bibliotecas para el préstamo bibliotecario.
Toda la información de carácter personal utilizada en esas aplicaciones reside en ellas y no puede ser accedida salvo desde la propia aplicación y previa autenticación del usuario, salvo la fotografía que para su representación ambas aplicaciones utilizan la técnica de URLs estáticas (direcciones web predeterminadas para cada fotografía y la misma para todas las consultas de cada foto), externas a la propia aplicación y a las que se accede mediante su indexación con un dato, para lo cual la Universidad de Zaragoza utilizó el número de identificación personal de cada universitario.
En estas circunstancias y a pesar de que las aplicaciones informáticas no permiten que se pongan restricciones en el acceso a las direcciones web (URL's) de las fotografías, estas direcciones no pueden considerarse como "públicas" en sentido amplio puesto que no son conocidas y sólo pueden obtenerse una vez accedido a la aplicación analizando el código fuente de sus páginas.
e) Análisis del incidente:
En los puntos anteriores se ha descrito la vulnerabilidad técnica que permitió que se desarrollara la página web de Lycos. Cuya consecuencia inmediata, como ya se ha dicho, fue la supresión de las páginas web que contenían la fotografía sin restricciones de acceso con lo que las fotografías dejaron de verse en la página de Lycos y en ambas aplicaciones informáticas (WebCT y Milenium).
Hay constancia del acceso a las fotografías el día 22 de febrero y se suprimió ese mismo día apenas 1 hora después de conocer el hecho.
El único dato al que pudo accederse desde la página web de Lycos fue al de la fotografía. Ni por el mecanismo utilizado para visualizar la fotografía ni por ningún otro del que se tenga constancia se pudo (ni se puede) acceder a otros datos personales sin previa identificación y autenticación. >>

TERCERO: Con fecha 20 de enero de 2009**,** el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a la Universidad de Zaragoza por la presunta infracción del

artículo 9 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.h) de dicha norma.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, en fecha 20/02/09 tiene entrada en esta Agencia, escrito de alegaciones de la Universidad de Zaragoza en el que, en síntesis, manifestaba que: 4/11

<<…El incidente sólo pudo originarse por la intervención de una persona que fuera usuaria y con amplios conocimientos de informática hasta el punto de ser capaz de decodificar, extraer códigos fuente y realizar un nuevo programa al que incorporarlos.
Estas acciones de pirateo informático son muy difíciles de impedir dado el estado actual de la tecnología y los avances que diariamente se producen en ella.
Aún así, las medidas de seguridad aplicables en la Universidad de Zaragoza:
a) Permitieron detectar la incidencia prácticamente desde el mismo momento en que se produjo.
b) Impidieron que la acción pirata pudiera entrar en el Fichero de Estudiantes propiamente dicho y con ello que pudieran externalizarse otros datos.
c) Se han aplicado restricciones a las aplicaciones afectadas por esta acción y se han adoptado las medidas de índoles técnicas y organizativas necesarias para salvaguardar, en todo momento, la seguridad e integridad del Fichero…>>

QUINTO: Con fecha 25/02/09, se acordó por el Instructor del procedimiento la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, E/00738/2008, así como la documental aportada por la Universidad de Zaragoza.

SÉXTO: Con fecha 14 de abril de 2009, 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 Universidad de Zaragoza ha infringido lo dispuesto en el artículo 9 de la LOPD, lo que supone una infracción tipificada como grave en el artículos 44.3.h) 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 del artículo 9 de la mencionada Ley.

HECHOS PROBADOS

PRIMERO: Con fecha de 3/3/2008 tiene entrada en esta Agencia escrito de D. X.X.X. en el que denuncia a la Universidad de Zaragoza, poniendo de manifiesto los siguientes hechos (folios 1 a 5):

<<PRIMERO: Que el día 21 de Febrero de 2008 tuve conocimiento a través de la página web www...Z... de una información de un usuario en la que explicaba la falta de seguridad de la Universidad de Zaragoza en la protección de los datos de los estudiantes. 5/11
SEGUNDO: En esta información, se señala que a través de la página web http://...Y...../...../..... se pueden obtener las fotografías de los expedientes de aquellas personas relacionadas con la Universidad de Zaragoza.
TERCERO: Tras escribir mi NIP (identificador único de la Universidad de Zaragoza) en la página web http://...Y...../...../..... ha aparecido mi fotografía. Esta fotografía es la misma que aporte en su día al matricularme a la Universidad de Zaragoza…>>

SEGUNDO: La Universidad de Zaragoza ha comunicado que:

<< a) - La página web a la que se hace referencia en el escrito de la Agencia de Protección de Datos (http://...Y...../...../.....) no pertenece al dominio de direcciones de la Universidad de Zaragoza, pertenece a la empresa LYCOS España Internet Services S.L.
Que no ha habido ninguna cesión de datos a dicha empresa.

Que conocido el incidente al que se hace referencia en el escrito de la Agencia de Protección de Datos, y que más adelante se detallará, se procedió de inmediato a solucionar el problema quedando resuelto en apenas 60 minutos.
Ni por el mecanismo utilizado para visualizar la fotografía en el incidente que se analiza ni por ningún otro del que se tenga constancia se pudo (ni se puede) acceder a ***otros*** *datos personales sin previa identificación y autenticación.*
Se tomaron las medidas necesarias para que no pueda volver a suceder una situación similar a la que posibilitó el incidente que se trata.
b) La Universidad de Zaragoza al realizar la matrícula en cualquiera de sus Centros solicita a todos sus estudiantes una fotografía que se incorpora al expediente del alumno y se utiliza tanto para su gestión docente como para su participación en las actividades y servicios de la universidad. Dicho documento gráfico tiene como finalidad el poder relacionar a la persona que solicita cualquier servicio de la Universidad, con los datos que dicha persona presenta.
La utilización de dichos documentos gráficos a través de páginas web es un procedimiento normalizado en algunos programas comunes en las Universidades que utilizan esas aplicaciones como son, en la Universidad de Zaragoza:
• WebCT, programa comercial específico para la enseñanza virtual (e-leaming).
• Milenium, programa de gestión de bibliotecas.
• Sigma, programa dedicado a la gestión académica.
c) El día 22 de febrero de 2008 se tuvo conocimiento de la existencia de la página web de Lycos (http://...Y...../...../.....). En ella introduciendo 6 dígitos se obtenía, en algunas ocasiones, la fotografía de una persona; única y exclusivamente la imagen sin ningún otro dato que pudiese identificarla y/o posibilitar su puesta en 6/11
relación con otros datos de carácter personal.
Se visualizaba una fotografía cuando el número introducido coincidía con lo que en la Universidad de Zaragoza se denomina NIP (número de identificación personal, asignado seriadamente a los alumnos de la universidad al matricularse). Se visualizaba la fotografía del estudiante cuyo NIP coincidía con esos dígitos.
Contrastada esta situación el día citado, a los 60 minutos de tener constancia del acceso indebido a las fotografías se suprimió el servicio y dejaron de visualizarse en Lycos las fotografías.
d) El origen del incidente se sitúa en las aplicaciones informáticas antes citadas: WebCT (aplicación para la enseñanza virtual) y Milenium (gestión de fondos bibliotecarios).
En la aplicación de gestión académica Sigma (tercera aplicación citada antes que utiliza las fotografías) se pudo utilizar una técnica diferente para la visualización de las fotografías que ***impedía*** *el problema.*
En ambas aplicaciones se accede a información personal previa identificación y autenticación de cada uno de los usuarios. Y a cada usuario se le muestra sólo la información pertinente: en WebCT (enseñanza virtual) a los profesores se muestra la ficha de sus estudiantes y a cada estudiante a su propia ficha; en Milenium se muestra a los gestores de las bibliotecas la información pertinente de los usuarios de las bibliotecas para el préstamo bibliotecario.
Toda la información de carácter personal utilizada en esas aplicaciones reside en ellas y no puede ser accedida salvo desde la propia aplicación y previa autenticación del usuario, salvo la fotografía que para su representación ambas aplicaciones utilizan la

técnica de URLs estáticas (direcciones web predeterminadas para cada fotografía y la misma para todas las consultas de cada foto), externas a la propia aplicación y a las que se accede mediante su indexación con un dato, para lo cual la Universidad de Zaragoza utilizó el número de identificación personal de cada universitario.
En estas circunstancias y a pesar de que las aplicaciones informáticas no permiten que se pongan restricciones en el acceso a las direcciones web (URL's) de las fotografías, estas direcciones no pueden considerarse como "públicas" en sentido amplio puesto que no son conocidas y sólo pueden obtenerse una vez accedido a la aplicación analizando el código fuente de sus páginas.
f) Análisis del incidente:
En los puntos anteriores se ha descrito la vulnerabilidad técnica que permitió que se desarrollara la página web de Lycos. Cuya consecuencia inmediata, como ya se ha dicho, fue la supresión de las páginas web que contenían la fotografía sin restricciones de acceso con lo que las fotografías dejaron de verse en la página de Lycos y en ambas aplicaciones informáticas (WebCT y Milenium). 7/11
Hay constancia del acceso a las fotografías el día 22 de febrero y se suprimió ese mismo día apenas 1 hora después de conocer el hecho.
El único dato al que pudo accederse desde la página web de Lycos fue al de la fotografía. Ni por el mecanismo utilizado para visualizar la fotografía ni por ningún otro del que se tenga constancia se pudo (ni se puede) acceder a otros datos personales sin previa identificación y autenticación… >> (folios 42 a 44).

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

La LOPD en sus art. 1 y 2.1) establece:
"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar."
"1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado."

III

Entrando en el análisis de las cuestiones de fondo planteadas en el presente procedimiento sancionador, 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. 8/11
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".
El citado artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.
Para poder delimitar cuáles son los accesos que la LOPD 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 a los ficheros el art. 3.a) los define como *"todo conjunto organizado de datos de carácter personal"* con independencia de la modalidad de acceso al mismo. Por su parte, la letra c) del mismo artículo 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"conservación"* o *"consulta"* de los datos personales tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.
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 conservación 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 refiere 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.
Partiendo de tales premisas deben analizarse a continuación las previsiones que el Real Decreto 994/1998, de 11 de junio, vigente en el momento de producción de la infracción, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, que continuaba en vigor de acuerdo con lo estipulado en la disposición transitoria tercera de la LOPD, prevía para garantizar que no se produzcan accesos no autorizados a los ficheros.
El artículo 2.10 del citado Reglamento de Seguridad considera *"soporte"* al *"objeto físico susceptible de ser tratado en su sistema de información sobre el cual se pueden grabar o recuperar datos"*. El precepto no distingue entre soportes informáticos o no, sino que resulta omnicomprensivo de todos ellos en congruencia con los preceptos de la LOPD ya expuestos, que tratan de evitar accesos no autorizados a los datos cualquiera que sea el procedimiento u operación para llevarlo a cabo.
El artículo 8 de dicho Reglamento de seguridad establece:
"1. El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información.
2. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.
3. El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
4. El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal".
Así, la Universidad de Zaragoza estaba 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 a los datos contenidos en tales ficheros por parte de terceros. Sin embargo, ha quedado acreditado que incumplió esta obligación, al no proteger adecuadamente en sus servidores web los ficheros en los que se almacenaban las fotografías de sus alumnos, siendo el NIP (conocido en el ámbito universitario) el único requisito necesario para poder acceder a éstas.

IV

El artículo 44.3.h) de la LOPD, considera infracción grave:
"Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".
De acuerdo con la disposición transitoria tercera de la LOPD, *"hasta tanto se lleven a efecto las previsiones de la Disposición Final Primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo, 1332/1994, de 20 de junio y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley"*.
Si bien la Universidad de Zaragoza mostró una notable diligencia para subsanar la incidencia detectada, existió vulneración del *"principio de seguridad de los datos"*, por lo que se considera que la Universidad de Zaragoza incurrió en la infracción grave descrita.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DECLARAR que la **UNIVERSIDAD DE ZARAGOZA** ha infringido lo dispuesto en el artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de de la citada Ley Orgánica.

SEGUNDO: NOTIFICAR la presente resolución a la **UNIVERSIDAD DE ZARAGOZA** y a **D. X.X.X.**.

TERCERO: 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 11/11
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.

Procedimiento Nº AP/00091/2009

RESOLUCIÓN: R/00835/2010

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00091/2009**, instruido por la Agencia Española de Protección de Datos a la entidad ***INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA"***, vista la denuncia presentada por varios denunciantes, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fechas 13 y 18 de marzo y 3 de abril de 2009, tuvieron entrada en esta Agencia escritos de ocho denunciantes, en los que denuncian que el Instituto de Enseñanza Secundaria "El Pla" de Alicante (en lo sucesivo IES "El Pla") ha instalado cámaras de videovigilancia que capturan imágenes y que incumplen la normativa de protección de datos.

En su escrito los denunciantes manifiestan lo siguiente: *"Que desde el día 3 de marzo de 2009, hay cámaras de videovigilancia instaladas en todos los pasillo del ÍES "El Pla", grabando sin cumplir con el deber de informarlo de forma pública a todos los interesados y afectados, sin inscribir los ficheros obligatorios en la Agencia de Protección de Datos, sin que se haya publicado en el Díario Oficial de la Generalitat Valenciana, pese a tratarse de un fichero de titularidad pública y sin que se hayan respetado los derechos de los interesados (profesores y alumnos). Además, a consecuencia de la instalación de las cámaras, un profesor del Instituto de Enseñanza Secundaria "El Pla" fue detenido el 4 de marzo por desinstalar las cámaras y, tras pasar dos días en los calabozos de comisaría, ahora está en libertad provisional en espera de juicio, acusado de presunto hurto, siendo las cámaras la prueba, e! motivo, y el fin de su detención. Esta grabación, realizada en el instituto el día 3 de marzo, pasó primero a manos de la Policía Nacional (Comisaría Distrito Norte de Alicante) y en la actualidad está en El Juzgado de Instrucción N°0A de ..... ".*

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicitó información al INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA" de Alicante, teniendo conocimiento de lo siguiente:

1.- Solicitada información al IES "El Pla" de Alicante, los representantes de la entidad manifestaron lo siguiente:

1. La instalación de un sistema de videovigilancia fue aprobada por unanimidad en sesión de Consejo Escolar del Centro el día 14 de enero de 2009. Se aporta certificado.
2. Se aporta copia de la contestación de la Delegación de Gobierno en Murcia, en relación con la instalación de un sistema de videovigilancia en el IES "El Plá".
3. Las cámaras están distribuidas de la siguiente forma:

- 13 Cámaras interiores:
o 1 hall principal
o 1 pasillo administración
o 1 pasillo sala profesores y talleres tecnología
o 1 hall planta primera
o 5 pasillos planta primera
o 4 pasillos planta segunda
- 4 cámaras exteriores:
o 1 entrada principal
o 1 aparcamiento motos alumnos
o 1 esquina derecha del patio

o 1 esquina izquierda del patio
4. Se aporta copia del modelo de cartel informativo de la existencia de cámaras. Existen 8 carteles informativos distribuidos por todo el Centro entre los que destacan los que se sitúan en las puertas de acceso principal
5. Respecto del formulario informativo que debe estar a disposición de los ciudadanos según se recoge en el artículo 3.b de la Instrucción 1/2006 y del procedimiento establecido para distribuir los formularios ante una petición del mismo, el representante de la entidad no se manifiesta, ni aporta copia de los formularios.
6. La empresa de seguridad que ha realizado la instalación del sistema de videovigilancia es ALARMAS MURCIA SISTEMAS Y SERVICIOS, S.L. inscrita en el Registro de Empresas de Seguridad de la Dirección General de la Policía con el número ****.
Se aporta copia del libro Catálogo de Instalaciones y Revisiones de la Jefatura Superior de la Policía.
7. El visionado en directo de las cámaras se realiza:
- Puerta principal: conserjes
- Resto cámaras: jefatura de estudios y directora
La Unidad Central del equipo de videovigilancia se encuentra custodiada en el despacho de la dirección del Centro, éste dispone de un disco duro que graba las imágenes por un periodo de 15 días, tras lo que procede a grabar encima de las imágenes anteriores.
El representante de la entidad manifiesta que *"No existen ficheros de las grabaciones dado que no se realiza un almacenamiento y clasificación de las imágenes."*
2.- Por parte de la Inspección de Datos se ha verificado lo siguiente:
 El Registro General de Protección de Datos ha comunicado que, a fecha 24 de agosto de 2009, no consta ningún fichero inscrito de video vigilancia inscrito en el Registro General de Protección de Datos en el que figure INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA" o Consejería de Educación de la Comunidad Valenciana.
 El IES "El Pla" no aporta copia del contrato de prestación de servicios suscrito con la entidad ALARMAS MURCIA SISTEMAS Y SERVICIOS, S.L.
 Tampoco aporta copia de la documentación acreditativa de que la empresa de seguridad instaladora está autorizada por el órgano administrativo competente del Ministerio del Interior como empresa de seguridad privada.

TERCERO: De los escritos de denuncia y de las actuaciones practicadas se desprende que el sistema de videovigilancia instalado en el INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA", podría incumplir el principio de proporcionalidad establecido en la Instrucción 1/2006 de Videovigilacia. Asimismo, se ha verificado la falta de inscripción del fichero de videovigilancia en el Registro General de Protección de Datos.

CUARTO: Con fecha 9 de diciembre de 2009**,** el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas al INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA" por las presuntas infracciones de los artículos 6 y 20 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.d) y 44.3.a) de dicha norma.

QUINTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, en fecha 7 de enero de 2010, el IES "EL PLA" presentó escrito de alegaciones en el que manifestaba lo siguiente:

1.- Que no es cierto que los denunciantes, todos ellos profesores del IES “EL PLA” no tuvieran conocimiento del sistema de videovigilancia en el momento de su instalación, el día 3 de marzo de 2009, puesto que “*en fecha 14 de enero de 2009, el Consejo Escolar del ÍES El Plá, adoptó por unanimidad la instalación de cámaras de vídeo vigilancia, del que forman parte los representantes del profesorado, elegidos por el claustro de profesores, y por tanto ostentan su representación en el máximo órgano de participación de los diferentes sectores de la Comunidad Educativa en el gobierno del ÍES El Plá”.*

2.- Que el centro docente dispone de ocho carteles informativos distribuidos por todo el centro y colocados en lugares suficientemente visibles y que dichos carteles o distintivos igualmente cumplen los requisitos establecidos en el Anexo de la Instrucción 1/2006.

Asimismo, adjuntan el formulario informativo que desde la instalación de las cámaras se encuentran a disposición de cualquier persona interesada en la Secretaría del Centro en el que se detalla la información prevista en el punto 3 apartado b) de la Instrucción 1/2006.

3.- *“En cuanto a la inscripción de fichero obligatorio en la Agencia de Protección de Datos, sin publicación en el diario oficial, con presunta vulneración del art. 20 de la LOPD, y art. 7. 1, de la Instrucción 1/2006, no se ha aprobado por el Consejo Escolar del centro, ni se ha comunicado a la Consellería de Educación ni a la Agencia de Protección de Datos, la creación de fichero, ya que el objeto de la instalación de las cámaras no tiene esta finalidad, en el presente caso, el sistema de videoviailancia consiste exclusivamente en la reproducción o emisión de imágenes en tiempo real, por tanto no se crean ficheros, todo ello de acuerdo con lo establecido en el art.7.2, de la precitada Instrucción 1/2006, que establece lo siguiente: ".no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real" A tenor de lo anterior, no puede ni debe constar ningún fichero inscrito de videovigilancia en el Registro General de Protección de Datos en el que figure el Instituto de Secundaria "El Plá", ya que las cámaras instaladas no almacén imágenes, limitándose a su reproducción en tiempo real, teniendo como único fin la seguridad en las personas que componen la comunidad educativa, todo ello al amparo de lo dispuesto en los artículos 3 y 7.2 de la Instrucción 1/2006, constituyendo por tanto un tratamiento de datos que obliga a informar del mismo, pero que no genera ningún fichero”.*

4.- En cuanto al principio de proporcionalidad: *“…El Consejo Escolar del centro adoptó por unanimidad, el acuerdo de la instalación de las cámaras como medida disuasoria y para prevenir situaciones que se venían produciendo con regularidad como:*

- Actos vandálicos, robos, destrozos de mobiliario del Centro y el inmueble.

- Extorsiones y amenazas entre alumnos. Menudeo y consumo de estupefacientes.

- Agresiones, peleas y acoso escolar.

- Destrozos de los sistemas de seguridad anti-incendios (rotura de extintores, mangueras y puerta cortafuegos).

No resulta ocioso señalar la responsabilidad que tienen encomendada los centros educativos sobre los alumnos que exige una continuada guarda de sus bienes y derechos durante el tiempo el lectivo, y que con las medidas adoptadas por el Instituto "El Plá" con la instalación de las cámaras de videovigilancia, se están protegiendo de manera mucho más eficaz, efectiva y diligente los mismos, consiguiéndose con ello la finalidad perseguida, es decir, que el Centro Docente sea mucho más seguro para todos sus integrantes, y puedan desarrollar con la mayor normalidad posible el desarrollo público de la enseñanza.

Por todo ello podemos afirmar que la instalación de las cámaras de vídeo vigilancia es una medida proporcional y justificada al cumplirse los siguientes requisitos:

1.- Las cámaras han conseguido reducir, y en muchos casos evitar las conductas que se estaban produciendo en el centro, constitutivas de delitos, faltas penales o infracciones administrativas, por tanto están cumpliendo el objetivo propuesto.
2.- La adopción de medidas para controlar, reducir o evitar las conductas precitadas hasta la instalación de las cámaras, no han resultado lo suficientemente eficaces para conseguir la seguridad en el centro, estando debidamente acreditado que tras su instalación se ha conseguido bastantes logros en relación al fin perseguido, es decir, que el Instituto de Enseñanza Secundaria sea un centro mucho más seguro para todos sus integrantes.
La captación de las imágenes en los pasillos del centro, y del patio, que son zonas de paso y de tiempo de recreo y no en los despachos, clases u otras dependencias del Instituto reduce considerablemente la posibilidad de obtener imágenes relativas a la intimidad de las personas, habiéndose limitado la zona de vigilancia a aquellos espacios más proclives a producirse los hechos o comportamientos constitutivos de infracciones administrativas o delitos penales. Dicha medida produce muchas más ventajas o beneficios que perjuicios tanto a los menores, profesorado y demás personas del centro, al ampliarse las garantías de seguridad de las personas y de sus bienes".
Adjunto a sus alegaciones el IES "EL PLA" aportó los siguientes documentos:
- Copia compulsada del contrato de prestación de servicios suscrito con la entidad ALARMAS MURCIA SISTEMAS Y SERVICIOS, S.L..
- Copia compulsada la documentación acreditativa de que la empresa de seguridad instaladora está autorizada por el Ministerio del Interior como empresa de seguridad privada.
- Copia compulsada la solicitud de autorización para la instalación del sistema de seguridad a la Delegación del Gobierno de Murcia, con motivo de la seguridad en el centro educativo en casos de hurto, atraco y robo.
- Copia compulsada de la resolución de autorización de dicho órgano administrativo.

SEXTO: Con fechas 4, 5, 7, 8 y 11 de enero de 2010, los denunciantes presentaron escrito de alegaciones en el que manifestaban lo siguiente:
1 "En relación a la información aportada por la directora del ÍES "El Pía" en el sentido de que la instalación del sistema de videovigilancia fue aprobada por unanimidad en sesión de Consejo Escolar del Centro el día 14 de enero de 2009, y como justificación de la cual aportó certificado, pongo en su conocimiento que, por las informaciones recibidas de representantes del profesorado en el Consejo Escolar presentes en dicha sesión, no se produjo ninguna votación para decidir la instalación del sistema.
Las cámaras de videovigilancia se instalaron en los pasillos del ÍES "El Pía" sin que los afectados hubiésemos recibido información en los términos previstos en el artículo 5 de la Ley Orgánica 15/1999 de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD), ya que los carteles que se colocaron en esa fecha no contenían la información que prescribe la ley; tampoco se disponía del formulario informativo que debía estar a disposición de los interesados, según se recoge en el artículo 3.b de la Instrucción 1/2006 (Se adjuntan fotografías del cartel tomadas en las fechas del 6 de marzo y 29 de mayo y 21 de diciembre :
Documento 1). Tampoco se nos proporcionó información concreta hasta el claustro celebrado el 8 de abril de 2009 —más de un mes después de la instalación y del comienzo de las grabaciones—, y así consta en el punto 2 del orden del día: "Información sobre sistema de videovigilancia. En este claustro la Directora del instituto hizo caso omiso de las intervenciones de varios profesores en las que se explicaban los graves incumplimientos de la LOPD (Se adjunta fotocopia del acta de dicho claustro y del escrito de don A.A.A. anexo a la misma).

2 Tampoco habían sido informados ni los alumnos del centro —muchos de ellos menores de edad— ni sus padres (Se adjunta fotocopia de la carta de una alumna del instituto publicada en el Díario Información el día 10 de marzo de 2009).
3 La instalación de cámaras y el comienzo de las grabaciones sin haberse respetado los cauces legales fueron el detonante para que nuestro compañero …. retirara algunas de esas cámaras el día 3 de marzo de 2009.
4 Las grabaciones obtenidas fueron utilizadas por la directora del instituto y por la policía para detener a …, lo cual tuvo graves consecuencias para él.
5 *Desde el comienzo de las grabaciones está siendo vulnerado mi derecho a la intimidad, así como el de mis alumnos, tanto en las zonas comunes como en aquellas aulas que pueden ser grabadas por las cámaras a través de ventanas y tabiques cuya parte superior es de cristal.*
6 Desde que las cámaras se instalaron nos sentimos indefensos, vigilados de manera injustificada y sometidos a una presión que ha ido en aumento. De hecho, se nos sigue grabando sin que sepamos exactamente el número y ubicación de las cámaras, y sin que, a fecha de hoy, tengamos conocimiento alguno de la finalidad de las grabaciones, ni del tratamiento de los ficheros que se generan, lo que impide el ejercicio de nuestros derechos de acceso, rectificación, cancelación y oposición. Y todo ello a pesar de las sucesivas advertencias que la directora ha recibido por parte de profesores, de sindicatos, de alumnos y de la propia Agencia.
7 Además, la imagen del centro y de los profesores ha resultado gravemente dañada, y todo ello como consecuencia de la incapacidad de la directora de gestionar la situación.
8 También nos sentimos perjudicados porque el elevado coste económico de la instalación, que consideramos innecesaria por desproporcionada, impide disponer de esos fondos para fines pedagógicos y didácticos mucho más urgentes.
9 En cuanto al volumen de los tratamientos efectuados, debemos recordar que las grabaciones afectan a más de cien profesores, más de mil alumnos, a todos sus padres, al personal no docente y a todas aquellas personas que utilizan las instalaciones del centro.
10 A pesar de que desde septiembre se han incorporado muchos alumnos y profesores nuevos, la dirección del centro no ha informado ni a los alumnos, ni a sus padres, ni a los profesores de las grabaciones que se llevan a cabo, ni de los derechos que como afectados tienen, lo cual podría ser considerado como una reincidencia en los puntos 2 y 3 del presente escrito.
11 En lo que respecta a la seguridad del centro, la realidad ha demostrado que el sistema de videovigilancia no evita que se produzca ocasionalmente —igual que antes de la instalación de dicho sistema— algún incidente de vandalismo o robo.
De hecho, durante el primer trimestre de este curso se produjo un acto de vandalismo contra las instalaciones del centro sin que las grabaciones efectuadas por las cámaras sirvieran para el esclarecimiento de los hechos. Por ello insistimos en el incumplimiento del principio de proporcionalidad establecido en la Instrucción 1/2006 de Videovigilancia.
12 *Por último, considero mi obligación como profesora reiterar que me parece particularmente grave la grabación de imágenes en el interior del instituto, precisamente porque se trata de un centro educativo en el que la mayoría de los alumnos es menor de edad y que tiene como una de sus finalidades primordiales la de formar a nuestros alumnos y educarlos en la responsabilidad, finalidad que, en mi opinión, difícilmente se logrará mientras se siga utilizando el sistema de videovigilancia"*

SÉPTIMO: Con fecha 12 de enero de 2010, la Consellería de Educación de la Generalitat Valenciana manifestó su intención de personarse como interesada en el procedimiento y presentó alegaciones en las que manifestó lo siguiente:

"PRIMERA.- El Decreto 234/1997, de 2 de septiembre, del Gobierno Valenciano, por el que se aprueba el Reglamento Orgánico y Funcional de los Institutos de Secundaria (D.O.G.V núm. 3.073, de 8 de septiembre de 1997), establece en su artículo 1 y 3 establece la dependencia de los institutos de la Consellería de Educación y la titularidad de la Generalitat Valenciana.
Por tanto, el ÍES "El Plá" de Alicante, es un centro público cuya titular es la Generalitat Valenciana y con dependencia de la Consellería de Educación.
SEGUNDA.- De conformidad con el art. 28 del Decreto 118/2007, de 27 de julio, del Consell, por el que se aprueba el Reglamento Orgánico y Funcional de la Consellería de Educación (D.O.C.V. núm: 5566, de 30 de julio de 2007):
"1.- Al frente de cada dirección territorial está el director territorial de Educación, con el carácter de representante permanente de la Consellería en el respectivo territorio.
2.- A los titulares de las direcciones territoriales les corresponde la jefatura de todos los servicios, programas y actividades que desarrollan los órganos, unidades y centros dependientes o integrados en la dirección territorial Con base a lo anterior este órgano territorial ostenta la jefatura de todas las actividades desarrollados en los centros docentes no universitarios en el ámbito territorial de Alicante, entre ellos se encuentra el ÍES "El Pía", de Alicante, y por tanto tiene la condición de interesado.
TERCERO.- En la resolución de referencia, el Director de la Agencia Española de Protección de Datos (en adelante AEPD) acuerda iniciar un procedimiento de declaración de infracción de las Administraciones Públicas, por la presuntas infracciones de los artículos 20 y 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD). Asimismo, indica que las presuntas infracciones vienen tipificadas en el art. 44.3.a), la primera, y 44.3, d) la segunda, de manera que se trata de dilucidar se ha incurrido, en los tipos siguientes:
"Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para ¡os mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario Oficial correspondiente ".
La primera de ellas, Y la segunda:
"Tratar los datos de carácter personal y usarlos posteriormente con conculcación de los principios y garantías establecidas en la Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituyan infracción muy grave ".
CUARTA.- En el hecho primero de resolución, se hace constar que las actuaciones practicadas tienen su origen en virtud de denuncia presentada con fechas 13 y 18 de marzo y 3 de abril de 2009, ante la AEPD por ocho denunciantes que manifiestan lo siguiente:
"Que desde el pasado día 3 de marzo de 2009, hay cámaras de videovigilancia instaladas en todos los pasillos del ÍES "El Pía", grabando sin cumplir con el deber de informarlo de forma pública a todos los interesados y afectados, sin inscribirlos ficheros obligatorios en la Agencia Española de Protección de Datos, sin que se haya publicado en el Diario Oficial de Generalitat Valenciana, pese a tratarse de un fichero de titularidad pública y sin que se hayan respetado los derechos de los interesados (profesores y alumnos)".
Recabada la información oportuna del citado Centro docente por este órgano se constata lo siguiente:
1º).- Los denunciantes, todos ellos profesores adscritos al ÍES "El Plá", tienen cumplida información de la instalación de las cámaras de videovigilancia, por varias fuentes de información, tanto a través del Consejo Escolar del Centro celebrado el 14 de enero de 2009, donde se aprobó por unanimidad la instalación de las cámaras, y del que forman parte además de los profesores que los representan por haber sido elegidos en elecciones a Consejos Escolares, los representantes de los padres, de los alumnos, el equipo directivo y el representante del personal de administración y

servicios, como de un Claustro de profesores celebrado con posterioridad a dicho Consejo.
2º).- Existen ocho carteles o distintivos informativos ubicados en lugares suficientemente visibles, tanto en espacios abiertos como en espacios como cerrados, resaltando los colocados en las puertas de acceso principal al edificio.
3º).- De igual manera el Centro docente tene a disp osición de los interesados en la Secretaría los impresos en los que se detalla la información prevista en el art. 5.1. de la Le Orgánica 15/1999.
A tenor de lo anterior, queda debidamente acreditado que lo expresado por los denunciantes en cuanto al deber de informar de forma pública a todos los interesados y afectados de la existencia de las cámaras de videovigilancia no se ajusta a verdad, por ser incierto e infundado.
QUINTA.- Con relación a lo expresado en la segunda parte de la denuncia sobre la inscripción de fichero obligatorio en la Agencia de Protección de Datos, sin publicación en el diario oficial, con presunta vulneración del art, 20 de la LOPD, y art. 7. 1, de la Instrucción 1/2006. Las cámaras instaladas en el ÍES "El Plá", tienen una única finalidad que no es otra que velar por la seguridad de la comunidad educativa, sin que exista ningún propósito o intención de crear fichero alguno, al no tener una organización o estar estructurado con arreglo a determinados criterios que permitan el tratamiento de datos, por tanto los datos captados no se almacenan en copias adicionales a las grabaciones, son recogidos y son borrados de forma automática por el propio dispositivo al sobreescribir encima de las imágenes captadas unos días antes, limitándose pues su reproducción a tiempo real.
En este sentido el art. 7, de la Instrucción de 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, cuando expresa la notificación de los
ficheros de titularidad pública es clara en redacción en su apartado 2° "A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real".
En este punto se trae a colación el contenido del informe del Gabinete Jurídico de la Agencia de Protección de Datos 2007/0212, que considera que la utilización de sistemas de videocámaras con fines de seguridad, que no graban imágenes, constituye un tratamiento de datos que obligan a informar del mismo, pero no generan ningún fichero.
Sin perjuicio de lo anterior este órgano se somete a cualquier consideración que pudiera expresar la Agencia sobre este extremo.
SEXTO.- En relación con la presunta infracción del art.44.3.d), al poder incumplir el principio de proporcionalidad establecido en la Instrucción 1/2006, se debe traer a colación el informe del Gabinete Jurídico de la Agencia de Protección de Datos 2006-0262 que considera una medida proporcional y justificada la implantación de sistemas de videovigilancia en los centros docentes, si se cumplen los siguientes requisitos:
I.- Que se trate de una medida susceptible de conseguir el objetivo propuesto.
2.- Que no exista otra medida más moderada para la consecución de tal propósito con igual de eficacia.
3.- Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.
La instalación de videocámaras en el ÍES "El Plá" de la ciudad de Alicante, tal y como se ha expresado con anterioridad, su único objeto es vigilar las distintas dependencias del centro escolar, por la obligación de defensa, protección y custodia del patrimonio de la Administración Pública y, también, por la atribución
de responsabilidad a los centros educativos sobre los alumnos y sobre los actos de éstos mientras se encuentran bajo la vigilancia o control del profesorado (téngase en cuenta que durante el horario lectivo tienen que desempeñar su labor docente con los menores, en sus funciones de vigilancia con la diligencia de un buen padre de familia).

Traemos a colación lo dispuesto en el artículo 1903 párrafo 5o, del Código Civil que determina lo siguiente " las personas o entidades que sean titulares de un centro docente de enseñanza no superior responderá por los daños y perjuicios que causen a sus alumnos menores de edad durante los periodos de tiempo en que los mismos se hallen bajo control o vigilancia del profesorado del centro, desarrollando actividades escolares o extraescolares o complementarias".
Asimismo, lo dispuesto en materia de responsabilidad patrimonial de la Administración en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
Asimismo, los artículos 28 y 29 de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas determinaron que las públicas están obligadas a proteger y defender su patrimonio. A tal fin, protegerán adecuadamente los bienes y derechos que lo integran, procurarán su inscripción registral y ejercerán sus potestades administrativas y acciones judiciales que sean procedentes para ello. Por otra parte, los titulares de los órganos competentes que tengan a su cargo bienes o derechos del patrimonio del estado están obligados a velar por su custodia y defensa, en los términos establecidos en este título".

OCTAVO: Con fecha 12 de enero de 2010, 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/01390/2009, así como las denuncias presentadas por todos los denunciantes y su documentación y la documental aportada por el INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA", los documentos obtenidos y generados por los Servicios de Inspección ante el INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA", y el Informe de actuaciones previas de Inspección que forman parte del expediente E/01390/2009.
Asimismo, se dio por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio AP/00091/2009 presentadas por todos los denunciantes así como las alegaciones presentadas por el INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA", y la documentación que a ellas acompaña.
Por otra parte, la Instructora del procedimiento acordó solicitar al IES "EL PLA" la remisión a esta Agencia de la siguiente información y documentación:
- Copia del Acta del Consejo Escolar aprobando la instalación de cámaras de videovigilancia.
- Información sobre quién mantiene el sistema de videovigilancia instalado (empresa de seguridad, portero, administrador….).
- Información en la que se detalle qué personas pueden visualizar las imágenes obtenidas, descripción del sistema utilizado para grabar las imágenes y el tiempo de conservación de las mismas. Información relativa a si las imágenes obtenidas permiten identificar personas.
- Información sobre si las cámaras instaladas en el exterior capturan imágenes de la vía pública y, en caso afirmativo, qué espacio de vía pública es captado por las cámaras.
- Información sobre si las cámaras instaladas capturan imágenes del interior de las aulas.
- Información sobre la existencia de cámaras ocultas
- Información sobre la existencia de monitores en el local que permitan visualizar las imágenes captadas por las videocámaras.
En virtud de lo solicitado por la Consellería de Educación de la Generalitat Valenciana, con fecha 13 de enero de 2010, la Instructora del procedimiento acordó:
- Incorporar a efectos probatorios las alegaciones presentadas por la Consellería de Educación de la Generalitat Valenciana y su documentación.
- Reconocer la personación como interesado de la Dirección Territorial de Alicante.

Con fecha 20 de enero de 2010, tuvo entrada en esta Agencia escrito del IES “EL Pla” en el que respondía a la solicitud de información lo siguiente:

1. “Copia del Acta del Consejo Escolar aprobando la instalación de cámaras de video-vigilancia: se adjunta copia compulsada como documento 1.2. Información sobre quién mantiene el sistema de video-vigilancia instalado (empresa de segundad, portero, administrador....): el mantenimiento del sistema de video-vigilancia lo realiza la empresa "Alarmas Murcia1' mediante contrato anual renovable firmado con dicha empresa autorizada. Se adjunta copia compulsada de contrato de mantenimiento como documento 2.3. Información en la que se detalle qué personas pueden visualizar las imágenes obtenidas, descripción del sistema utilizado para grabar las imágenes y el tiempo de conservación de las mismas. Información relativa a si las imágenes obtenidas permiten identificar personas: el Centro está dotado con las siguientes cámaras de video-vigilancia. Se adjunta certificado de la empresa instaladora como documento 3: a. 1 cámara exterior que enfoca la entrada principal al recinto y que no está conectada al videograbador, por tanto el visionado se realiza en tiempo real y no se pueden reproducir las imágenes. El monitor de visionado está ubicado en la conserjería del Centro visualizado por los conserjes. Esta cámara vino instalada por la dotación del Centro a la recepción de la obra. b. 3 cámaras que enfocan los patios. El monitor de visionado se encuentra en el despacho de Jefatura de Estudios dónde se realiza el visionado en tiempo real: Una (1) cámara que enfoca permanentemente el parking de las motos de los alumnos. Dos (2) cámaras que hacen un visionado de barrido por los patios de recreo y las vallas del Centro (con la intención de vigilar las posibles fugas de alumnos o saltos de las vallas de personas ajenas al Centro, así como los trapicheos o menudeo de estupefacientes a través de las mismas). c. Trece (13) cámaras interiores distribuidas de la siguiente forma:

Una (1) en el hall principal

Una (1) en el pasillo de administración Una (1) en el pasillo planta baja

Una (1) en el hall de la planta primera Cinco (5) en los pasillos de la planta primera Cuatro (4)en los pasillos de la planta segunda Todas estas cámaras están conectadas a un videograbador de 16 canales provisto de un disco duro de 500 gígas, que se encuentra en el despacho de dirección. Se realiza el visionado de las cámaras en tiempo real mediante un monitor que se encuentra en el despacho de dirección. El videograbador conserva las imágenes durante 2 semanas, momento en el que automáticamente vuelve a grabar encima de las anteriores, no conservándose las grabaciones anteriores. No se descargan archivos de grabación para su almacenamiento ni se realiza ningún tipo de manipulación con las mismas, perdiéndose todos los datos al cabo de las 2 semanas.

Las cámaras interiores no disponen de zoom por lo que resulta dificultoso identificar a las personas, lo que se aprecian, en algunos casos, son las características y los colores de la vestimenta y si se está produciendo algún altercado, en un momento dado, por lo que se acude al lugar de los hechos para intentar resolverlo o identificar a las personas. En realidad la eficacia de las cámaras no reside en las imágenes que proporcionan sino en el carácter disuasorio de las mismas dado que el alumno/a desconoce la nitidez y calidad de la imagen.

4. Información sobre si las cámaras instaladas en el exterior capturan imágenes de la vía pública y, en caso afirmativo, qué espacio de vía pública es captado por las cámaras: las cámaras instaladas en el exterior y que realizan el visionado en barrido de las vallas del recinto capturan una parte mínima de las aceras del entorno al Centro con una visión muy lejana de las mismas donde resulta imposible identificar a personas.

5. Información sobre si las cámaras instaladas capturan imágenes del interior de las aulas: ninguna de las cámaras instaladas captura imágenes de las aulas ni de parte de

ellas, tampoco en aseos, vestidores, talleres o gimnasios. Todas las cámaras están situadas en pasillos y zonas comunes de paso.
6. Información sobre cámaras ocultas: no existe ninguna cámara oculta ni camuflada, todas las cámaras están perfectamente visibles ante cualquier miembro de la comunidad educativa.
7. Información sobre los monitores en el local que permitan visualizar las imágenes captadas por las video-cámaras:
a. Una (1) cámara exterior que enfoca la entrada principal al recinto. El monitor de visionado está ubicado en la conserjería del Centro visualizado por los conserjes.
b. Tres (3) cámaras que enfocan los patios. El monitor de visionado se encuentra en el despacho de Jefatura de Estudios.
c. Trece (13) cámaras interiores. El monitor de visionado se encuentra en el despacho de dirección".

NOVENO: Con fecha 24 de febrero de 2010, 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 el Archivo de las presentes actuaciones respecto de la infracción imputada del artículo 6 de la LOPD. Asimismo, que por el Director de la Agencia Española de Protección de Datos se declare que el INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA" ha infringido lo dispuesto en el artículo 20 de la LOPD, lo que supone una infracción tipificada como grave en el artículo 44.3.a) 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 del artículo 20 de la mencionada Ley.
El IES "EL PLA" no ha presentado, hasta la fecha, alegaciones frente a la citada propuesta de resolución.
Con fecha 30 de marzo de 2010, la Consellería de Educación de la Generalitat valenciana presentó alegaciones en las que manifestó lo siguiente:
"Primera.- Con relación al art. 6 de la LOPD, y con la única finalidad de que el órgano competente para dictar resolución recoja en la misma los hechos probados más ajustados por los que se debe fundamentar el archivo de la infracción imputada se expresa lo siguiente:
a).- El ÍES "El Plá" de Alicante, ha cumplido el principio de proporcionalidad establecido en el art. 4 de la Instrucción 1/2006 de Videovigilancia, al haberse ajustado la instalación de las cámaras de videovigilancia a satisfacer de manera exclusiva necesidades de seguridad del centro docente, frente a los actos vandálicos, robos, destrozos en el mobiliario y en el inmueble del centro, extorsiones y amenazas entre los alumnos, menudeo y consumo de estupefacientes, agresiones, peleas y acoso escolar.
Las conductas que se acaban de enumerar fundamentaron el Acuerdo del Consejo Escolar de 14 de enero de 2009, sobre la aprobación por unanimidad de la instalación de las cámaras, hecho que consta en la documentación recabada por la Sra. Instructora del presente procedimiento, no habiéndose desvirtuado la veracidad de las mismas por los denunciantes.
De igual manera, la Sra. Instructora del procedimiento tanto por lo alegado por este órgano como por la dirección del centro docente ha podido constatar y verificar de manera fehaciente las conductas descritas solicitando durante el periodo de prueba, tanto al centro docente como al Ministerio del Interior (Comisaría de Policía Distrito Norte de Alicante), así como al GRUME (Grupo de Menores de la Policía Autonómica) toda la documentación relativa a las precitadas conductas que han venido sucediéndose durante años.
En este punto conviene poner de manifiesto en relación con la instalación de sistemas de videocámaras, la Instrucción 1/2006, que hace referencia a la necesidad de

ponderar los bienes jurídicos protegidos, y que viene a señalar expresamente que la instalación de este tipo de dispositivos deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injusficadas en los derechos y libertades fundamentales.

El Tribunal Constitucional en su sentencia 207/1996, entre otras, ha señalado respecto de la proporcionalidad que se trata de "una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad".

En este sentido, hay que destacar que para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones:

1.- La medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad).

2.- La medida es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesariedad).

3.- La medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

En consecuencia, la instalación de cámaras de videovigilancia, debe reunir estos requisitos o condiciones. Es decir, que tal medida, debe ser idónea, necesaria y proporcional. No cabe duda que dichas medidas o requisitos en el presente caso se cumplen, al haberse conseguido con dicha instalación los objetivos perseguidos con la aprobación de su instalación, es decir, una mayor protección y seguridad tanto de los menores, como del resto de personas de la Comunidad Educativa, así como una mayor protección del patrimonio público de la Generalitat Valenciana, siendo susceptible de comprobación con los datos objetivos que tal y como se ha expresado, constan en las distintas fuentes señaladas con anterioridad. De igual manera no se ha aportado por los denunciantes ninguna otra medida más moderada para conseguir tal propósito con igual eficacia. En este sentido los datos precitados avalan dicha eficacia, y consta como dato objetivo fácilmente verificable que todas las medidas adoptadas por el centro docente desde su puesta en funcionamiento hace unos cuantos años, no han conseguido ni controlar ni minorar las conductas descritas. A modo meramente ilustrativo, y referido a los actos vandálicos, tras la instalación de las cámaras, y después de más de un año, consta un solo acto, aprovechando una parte del centro que no tiene cámaras, frente a las múltiples denuncias cursadas con anterioridad por estas conductas.

Finalmente, la medida es ponderada y equilibrada al haberse constatado que las cámaras de videovigilancia son un instrumento válido para la protección de todos los miembros de la Comunidad Educativa (bien jurídico vida, y la integridad de las personas) y los bienes públicos que permiten el ejercicio del derecho fundamental a la educación, derivándose de ello de forma clara y manifiesta beneficios y ventajas para el interés general, produciéndose por otro lado, un menoscabo mínimo en el derecho fundamental a la intimidad y a la propia imagen al estar ubicadas las cámaras en lugares de paso, pasillos, accesos de entrada y salida, patio, etc. (preservándose en todos los casos los espacios más íntimos).

b) .- El ÍES "El Plá" de Alicante ha cumplido con el deber de información a los afectados en los términos establecidos en el art. 3 de la Instrucción 1/2006, en relación con el art. 5.1 de la LOPD, al haberse aprobado por la unanimidad del Consejo Escolar la instalación dichas cámaras, y haberse instalado éstas 50 días después de la aprobación de dicho acuerdo. Asimismo, por haberse dispuesto en las zonas de emplazamiento de las cámaras con la señalización y advertencias correspondientes,

con carteles informativos de zona vigilada por video y de la identidad del ÍES "EL PLA", como responsable del fichero ante quien pueden hacerse efectivo sus derechos.
c) .- El ÍES "El Plá" de Alicante ha cumplido el art. 6, de la Instrucción 1/2006, al haber quedado debidamente acreditado que a los 15 días el disco duro que graba las imágenes, ubicado en el despacho de la dirección del centro, procede a grabar encima de las anteriores imágenes, por tanto respetándose el plazo de un mes fijado en la norma.
d) .- El ÍES "El Plá" de Alicante, no ha vulnerado el derecho fundamental a la intimidad y la propia imagen, al captar imágenes de alumnos, profesores y personal del centro cuando circulaban por las instalaciones escolares, con el único objetivo de preservar la seguridad de las personas y el patrimonio de la Generalitat Valenciana, y sin finalidad alguna de observar la vida intima de las personas. En este sentido de ha expresado la Sentencia del T.S. de 2 de julio de 2004. No obstante si las imágenes captadas hubiesen revelado elementos Íntimos o privados de las personas sí hubiera exigido extremarse las medidas de protección para evitar una vulneración de derechos, en particular los deberes de seguridad, secreto y confidencialidad que se imponen para la protección de esos datos. Por ello, un elemento muy valorado por el Tribunal Constitucional para determinar si existe o no, intromisión ilegítima es el hecho de que las imágenes no hayan sido publicadas ni reproducidas. Y es que la LO 1/1982, efectivamente no exige que la imagen deba ser publicada para considerar que existe intromisión, sin embargo el TC sí que ha configurado dicho requisito como elemento decisivo en muchas ocasiones. De hecho la mayor parte de las sentencias relativas a la vulneración de derecho a la intimidad o a la propia imagen se refieren a supuestos en los que las imágenes fueron publicadas en medios de comunicación. En el presente caso, no ha habido ningún tipo de publicación ni reproducción de ninguna de las imágenes captadas por las cámaras de videovigilancia del centro docente, por ello, no ha existido intromisión ilegítima del derecho fundamental a la intimidad y a la propia imagen.
Sin perjuicio de lo anterior, tal y como expresan los denunciantes, uno de ellos, fue detenido por las Fuerzas y Cuerpos de Seguridad, por un presunto delito de hurto, y los agentes de la autoridad solicitaron el auxilio necesario en la investigación de la sustracción de las cámaras para la persecución de los delitos. La Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, recoge en su art. 4, 1: " Todos tienen el deber de prestar a las Fuerzas y Cuerpos de Seguridad el auxilio necesario en la investigación y persecución de los delitos en los términos previstos legalmente". Y en su apartado 2, del mismo artículo: "Las personas o entidades que ejerzan funciones de vigilancia, seguridad, o custodia referidas a personas y bienes o servicios de titularidad pública o privada tienen especial obligación de auxiliar o colaborar en todo momento con las Fuerzas y Cuerpos de Seguridad"" De la documentación que obra en este órgano territorial consta que tras haberse instalado las cámaras el día 2 de marzo, se detectaron por el personal del centro al día siguiente la desaparición de 3 videocámaras, con rotura de la instalación del cableado. Dicho hecho motivó la oportuna denuncia ante la Comisaría de Policía, la cual con base a los preceptos citados con anterioridad solicitó y obtuvo de la dirección del centro las imágenes de las cámaras más próximas a las arrancadas para la averiguación y persecución del presunto delito cometido. Por tanto el único uso de las imágenes captadas ha sido el amparado por la citada L.O. 2/1986.
A modo de conclusión el archivo de la infracción imputada, amén de los considerandos efectuados por la Sra. Instructora del expediente, totalmente admisibles, respetables y ajustados a derecho, tienen su fundamento en todo lo expresado con anterioridad, que despeja cualquier duda sobre el cumplimiento del principio de proporcionalidad establecido en la Instrucción 1/2006 por el ÍES "El Plá" de Alicante en la puesta en funcionamiento del sistema de videovigilancia en dicho centro docente. Segunda.- Con

relación a la infracción de lo dispuesto en el art. 20 de la LOPD, por el ÍES "El Plá" de Alicante, se significa lo siguiente:
a) .- La Consellería de Educación por ORDEN de 25 de agosto de 2008 (D.O.G.V. n° 5844, de 8.09.2008) procede a la creación de ficheros de carácter personal de la Consellería de Educación, en los términos y condiciones fijados en la Ley Orgánica 15/1999, de protección de datos de carácter personal.
b).- Entre los ficheros creados figuran los siguientes: 1. ALUMNOS; 4. PERSONAL DOCENTE; 5. GESTIÓN ADMINISTRATIVA; 6. ALUMNOS EXTENDIDO; 7. GESTIÓN PATRIMONIAL; 8. PERSONAL DOCENTE EXTENDIDO.
c) .- Se señala en la citada Orden de 25 de agosto de 2008, el lugar ante el que se deberá ejercitar los derechos de acceso, rectificación, cancelación y oposición: Registro General de la Consellería de Educación.
d) .- En cuanto al tratamiento de los datos de los alumnos, la Ley Orgánica 2/2006, de educación, en su artículo 71 dispone: "Las Administraciones educativas dispondrán de los medios necesarios para que todo el alumnado alcance el máximo desarrollo personal, intelectual, social y emocional, así como los objetivos establecidos con carácter general en la presente Ley".
En la disposición Adicional vigésimo tercera de la Ley Orgánica 2/2006, de 3 de mayo de Educación (LOE) se establece en el apartado 1: "los centros docentes podrán recabar los datos personales de su alumnado que sean necesarios para el ejercicio de la función educativa. Dichos datos podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos".
En su apartado 2 se dice: "los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información a la que hace referencia este artículo. La incorporación de un alumno a un centro docente supondrá el consentimiento para el tratamiento de sus datos, y en su caso, la cesión de datos procedentes del centro en el que hubiere estado escolarizado con anterioridad, en los términos establecidos en la legislación sobre protección de datos.."
Lo mencionado lo reconoce en el Informe Jurídico 0399/2008 de la AEPD, que "De lo previsto en ambos aparados se desprende la existencia de una habilitación legal para el tratamiento por los centros educativos de los datos de los alumnos y de los relacionados con su entorno familiar y social que sean necesarios para el adecuado cumplimiento de su función educativa, descrita en el apartado 2 en sus vertientes educativa y orientadora": Aparece, por tanto, una habilitación legal para el tratamiento de los datos que excluye que el afectado o su representante legal otorgue el consentimiento para el tratamiento de cuantos datos sean necesarios para el desempeño de las funciones docente y orientadora.
No sólo excluye el consentimiento del alumnos y de sus padres o tutores para el tratamiento de los datos, sino que por el contrario les impone un deber de cooperación en la obtención y tratamiento de éstos que podrá ser invocado pro el Centro en el caso de existir resistencia a facilitar las citadas informaciones.
Corresponde llegado este punto hacer una interpretación del término descrito en la disposición adicional vigésimo tercera de la LOE "función educativa". La palabra "función" está definida por la Real Academia como "Tarea que corresponde realizar a una institución o entidad, o a sus órganos o personas". El adjetivo "educativa" se define como "perteneciente o relativo a la educación". Al tratarse de un derecho fundamental, la educación, la interpretación debería entenderse en un sentido amplio. En cualquier caso, dado que la AEPD ha abierto este expediente en el que de algún modo se dilucida como fondo de la cuestión el uso de ciertos medios (cámaras de seguridad) por parte de un Instituto, en el que su máximo órgano de representación

democrática (Consejo Escolar), entendió que favorecían la función educativa en una zona "socialmente muy problemática".
e) .- En cuanto a los denunciantes ….. en su condición de profesores y personal dependiente de la Consellería de Educación no consta que hayan efectuado escrito, queja, denuncia, ni cualquier otro tipo de reivindicación en relación con las cámaras de videovigilancia del centro ante esta Administración Educativa, sino que han acudido directamente a denunciar a la Agencia Española de Protección de Datos, actuación que por otro lado, está perfectamente ajustada a derecho. La denuncia cursada por los mismos, efectuada los días 13 y 18 de marzo y 3 de abril, guarda una clara y manifiesta relación causa-efecto con la actuación de uno de ellos, tal y como se ha expresado con anterioridad al intentar minimizar una conducta presuntamente delictiva llevada a cabo el 3 de marzo, con el cumplimiento por parte de un centro docente de los requisitos exigidos por la normativa expresa.
f) .- El ÍES "El Plá" de Alicante, cumplió con todas las formalidades exigidas tanto en la LOPD, como en la Instrucción 1/2006, para la instalación del sistema de videocámaras, salvo en lo referente a la interpretación del art. 7.2, de la citada Instrucción al considerar que el borrado automático en un plazo inferior a un mes del único disco duro existente ubicado en el despacho de la dirección, no generaba fichero, por lo que no se realizaron todas las actuaciones encaminadas al cumplimiento de los trámites del art. 20 de la LOPD. A tenor de lo anterior, por parte de este órgano territorial, y sin perjuicio de la resolución que se dicte en el presente expediente, va a proceder a dar traslado de todo lo actuado al Centro Directivo competente de la Consellería de Educación para el inicio de los trámites que correspondan para adecuar sus instalaciones al marco jurídico vigente. Por todo ello solicitó "*Que se tenga por formuladas las alegaciones contenidas en el cuerpo de presente escrito, se admitan, y se consideren los fundamentos expresados en la primera de ellas sobre el cumplimiento del principio de Proporcionalidad, a los efectos de su debida inclusión en la resolución"*

HECHOS PROBADOS

PRIMERO: Con fechas 13 y 18 de marzo y 3 de abril de 2009, tuvieron entrada en esta Agencia escritos de ocho denunciantes, en los que denuncian que el IES "EL Pla" de Alicante ha instalado cámaras de videovigilancia que capturan imágenes y que incumplen la normativa de protección de datos (folios 1-21).

SEGUNDO: La implantación de un sistema de videovigilancia en el IES "EL PLA" fue aprobada por unanimidad en sesión ordinaria del Consejo Escolar celebrada el día 14 de enero de 2009, constando en el desarrollo del punto 4 del orden del día del Acta levantada con motivo de tal sesión, relativo a: " *Revisión presupuestos cámaras de vigilancia",* que *"todos los miembros presentes del C. E. están de acuerdo en que se instalen cámaras de vigilancia*" (folios 247 y 250).

TERCERO: La instalación de cámaras de vigilancia en las dependencias del centro obedecía a razones de seguridad y vigilancia, ya que con tal medida se pretendía evitar los actos vandálicos y daños en bienes y personas que venían produciéndose en distintas zonas del instituto. Es decir se instaló como medida disuasoria y para prevenir situaciones que se venían produciendo con regularidad como *"actos vandálicos, robos, destrozos de mobiliario del Centro y el inmueble, extorsiones y amenazas entre alumnos, menudeo y consumo de estupefacientes, agresiones, peleas y acoso escolar, destrozos de los sistemas de seguridad anti-incendios (rotura de extintores, mangueras y puerta cortafuegos)"* (folios 123-125 y 331).

CUARTO: Consta acreditado que la empresa que instaló el sistema de videovigilancia, denominada ALARMAS MURCIA, S.L. figura inscrita como empresa de seguridad en el correspondiente registro del Ministerio del Interior con el número ****. La instalación consta autorizada por la Delegación del Gobierno (folios 37-46 y 129-137, entre otros)

QUINTO: En el momento de la entrada en funcionamiento del citado sistema, acaecido con fecha 3 de marzo de 2009, según la Directora del citado Instituto había un total de 17 cámaras distribuidas por diferentes dependencias de las plantas del Instituto: 13 Cámaras interiores: 1 hall principal, 1 pasillo administración, 1 pasillo sala profesores y talleres tecnología, 1 hall planta primera, 5 pasillos planta primera, 4 pasillos planta segunda, así como 4 cámaras exteriores: 1 entrada principal, 1 aparcamiento motos alumnos, 1 esquina derecha del patio y 1 esquina izquierda del patio. El visionado en directo de las cámaras se realiza de la siguiente forma:
- Puerta principal: conserjes
- Resto cámaras: jefatura de estudios y directora
La Unidad Central del equipo de videovigilancia se encuentra custodiada en el despacho de la dirección del Centro, éste dispone de un disco duro que graba las imágenes por un periodo de 15 días, tras lo que procede a grabar encima de las imágenes anteriores (folios 37 y 38, entre otros).

SEXTO: Las zonas del emplazamiento de las cámaras cuentan con la señalización y advertencia correspondiente. Los representantes del IES y de la empresa instaladora del sistema han aportado imágenes donde se observan carteles informativos de zona vigilada por vídeo y de la identidad del IES "EL PLA" como responsable del fichero ante quien pueden hacer efectivo sus derechos (folio 46, ….). Los denunciantes también han presentado copia de los carteles informativos, aunque no aparece mencionado el responsable del fichero (folios 99-101 y 228, entre otros).

SÉPTIMO: Consta acreditado que, en el momento de la denuncia el sistema de videovigilancia grababa imágenes y así lo han manifestado los representantes de la entidad en reiteradas ocasiones: *"dispone de un disco duro que graba las imágenes por un periodo de 15 días, tras lo que procede a grabar encima de las imágenes anteriores"* (folios 38, 44: videograbador, 50).
Incluso en el Acta nº 47/2009, del Claustro IES "EL PLA" de 8 de abril de 2009 se recoge: *"La Directora informa … cada mes se borran los datos*" (folio 167). También la Consellería de Educación manifiesta al respecto: *"los datos captados no se almacenan en copias adicionales a las grabaciones, son recogidos y borrados…. Al sobrescribir encima las imágenes captadas unos días antes"* (folio 229). Por último la Directora del IES manifiesta *"Todas las cámaras están conectadas a un videograbador… se realiza el visionado de las cámaras a tiempo real…el videograbador conserva las imágenes durante 2 semanas, momento en que automáticamente vuelve a grabar encima…perdiéndose todos los datos al cabo de dos semanas*" (folio 244).

OCTAVO: No consta acreditado que el sistema de videovigilancia capture imágenes de la vía pública, únicamente parece captar el espacio mínimo necesario de acceso al edificio (folios 109 y 145).

NOVENO: Con fecha 24 de agosto de 2009, no consta en el Registro General de Protección de Datos ningún fichero de vídeo vigilancia cuyo responsable sea el IES "EL PLA". Tampoco consta que el fichero de videovigilancia de titularidad pública creado cuente con autorización de *disposición general publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente",* ni consta que hasta la fecha, se haya procedido a la inscripción del citado fichero (folios 60-61).

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

Respecto de los hechos objeto de denuncia, hay que señalar, en primer lugar que el artículo 1 de la LOPD dispone: "*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*". La LOPD, viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.

En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado";* definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *"Cualquier información concerniente a personas físicas identificadas o identificables".*

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*". La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

El artículo 5.1. f) 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, define datos de carácter personal como: *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, 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 personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; 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"*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte,

la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.
La Directiva 95/46/CE en su Considerando 14 afirma: *"(14)Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;".*
Por tanto, la captación de imágenes con fines de vigilancia y control se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal. Este tratamiento de datos se encuentra regulado de forma específica en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en cuyo artículo 1 señala que la citada Instrucción "*se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras*" entendiéndose por tratamiento *"la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas*."

III

En primer lugar, se imputa al IES "EL PLA" la presunta comisión de una infracción del artículo 6 de la LOPD, que dispone lo siguiente:
"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos. 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".
Respecto a la legitimación en el tratamiento de las imágenes, la respuesta se encuentra en el artículo 2 de la Instrucción 1/2006, que establece que: *"1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. 2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y vídeocámaras deberá respectar en todo caso los requisitos exigidos por la legislación vigente en la materia".*

Para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: *"La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública".*
Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) es la Ley Orgánica 15/1999, donde se prevé que: *"Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*
e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia". En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, y además en el mismo texto legal se regulan los criterios para instalar las cámaras y los derechos de los interesados.
En el presente caso, si bien consta acreditada la existencia de varias cámaras en las instalaciones del IES "EL PLA" objeto de denuncia, debido a la imposibilidad de efectuar las comprobaciones precisas en el domicilio denunciado en el momento de la denuncia, no ha sido posible comprobar si las citadas cámaras captaban imágenes de la vía pública superando el principio de proporcionalidad establecido en la Instrucción 1/2006.
A este respecto hay que señalar que el IES imputado siempre ha manifestado que instaló el sistema de videovigilancia por motivos de seguridad y consta acreditado que lo hizo tras su aprobación por el Consejo Escolar. Por otra parte, también ha mantenido que las cámaras exteriores permitían una visualización y grabación de imágenes del espacio mínimo exigido para visualizar la entrada al edificio. En cuanto a las cámaras interiores, de la información y documentación que obra en el expediente, no se desprende que ninguna de ellas supere el citado principio de proporcionalidad ya que no consta acreditado que capturen imágenes del interior de las aulas, vestuarios ni espacios íntimos.
El Tribunal Constitucional ha declarado de forma reiterada que al Derecho Administrativo Sancionador le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta "*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".* De acuerdo con este planteamiento, 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 en lo sucesivo LRJPAC), establece 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."*

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la presunción de inocencia *"no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsución estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo."*

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate."*

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y acreditado una prueba de cargo acreditativa de los hechos que motivan la imputación o de la intervención en los mismos del presunto infractor, aplicando el principio *"in dubio pro reo"* en caso de duda respecto de un hecho concreto y determinante, que obliga en todo caso a resolver dicha duda del modo más favorable al interesado.

No obstante lo anterior, debe resaltarse que el Tribunal Constitucional, en su Sentencia 24/1997, tiene establecido que *"los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*

a) La prueba indiciaria ha de partir de hechos plenamente probados.

b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)." En el presente caso, consta acreditada la existencia de varias cámaras exteriores, alguna de ellas orientada hacia la vía pública. Sin embargo no se ha podido constatar que tales cámaras capten imágenes de la vía pública que superen el principio de proporcionalidad establecido en la Instrucción 1/2006, que exige la ponderación en cada caso entre la finalidad pretendida y la posible afectación de las videocámaras al derecho al honor, a la propia imagen y a la intimidad de las personas y requiere, por tanto, la existencia de un razonable riesgo para la seguridad ciudadana. A este respecto hay que señalar que el sistema se instaló como medida disuasoria y para prevenir situaciones que se venían produciendo con regularidad como *"Actos vandálicos, robos, destrozos de mobiliario del Centro y el inmueble, extorsiones y amenazas entre alumnos, menudeo y consumo de estupefacientes, agresiones, peleas y acoso escolar, destrozos de los sistemas de seguridad anti-incendios (rotura de extintores, mangueras y puerta cortafuegos)"* Por tanto, de acuerdo con los

principios señalados procede el archivo las presentes actuaciones respecto de la infracción del artículo 6 imputada.

IV

En segundo lugar, se imputa al IES "EL PLA" una infracción del artículo 20 de la LOPD que señala que:
"*1. La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o díario oficial correspondiente.*
2. Las disposiciones de creación o de modificación de ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo.
b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.
d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.
f) Los órganos de las Administraciones responsables del fichero.
g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.
h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.
3. En las disposiciones que se dicten para la supresión de los ficheros se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción"
En el presente caso, ha quedado acreditado que, desde el 3 de marzo de 2009, fecha en que el sistema de videovigilancia del IES "EL PLA" entró en funcionamiento, dicho IES utilizó el fichero de datos de carácter personal *"FICHERO DE VÍDEO VIGILANCIA"* sin que, hasta la fecha, dicho fichero haya sido inscrito en el Registro General de Protección de Datos.
Por lo tanto, está acreditado que el IES "EL PLA" creó un fichero de titularidad pública y procedió a iniciar la recogida de datos de carácter personal con anterioridad a la inscripción en el Registro General de Protección de Datos, conducta que supone la vulneración del artículo 20 de la LOPD.

V

En sus alegaciones al Acuerdo de Inicio el IES manifestó en su defensa que el sistema de videovigilancia no graba y que únicamente permite la visualización a tiempo real, no existiendo, por tanto, ficheros de datos personales ni obligación de declarar tales ficheros ante la Agencia Española de Protección de Datos. Sin embargo, consta acreditado que el sistema sí graba imágenes, a este respecto hay que señalar que durante las actuaciones previas de investigación, el IES manifestó lo siguiente: *"dispone de un disco duro que graba las imágenes por un periodo de 15 días, tras lo que procede a grabar encima de las imágenes anteriores. No existen ficheros de las grabaciones dado que no se realiza un almacenamiento y clasificación de las imágenes""* (folios 38, 44: videograbador, 50). Incluso en el Acta nº 47/2009, del Claustro IES "EL PLA" de 8 de abril de 2009 se recoge:
"La Directora informa … cada mes se borran los datos" (folio 167). También la Consellería de Educación manifiesta al respecto: *"los datos captados no se almacenan en copias adicionales a las grabaciones, son recogidos y borrados…. Al sobrescribir*

encima las imágenes captadas unos días antes" (folio 229). Por último la Directora del IES manifiesta *"Todas las cámaras están conectadas a un videograbador… se realiza el visionado de las cámaras a tiempo real…el videograbador conserva las imágenes durante 2 semanas, momento en que automáticamente vuelve a grabar encima…perdiéndose todos los datos al cabo de dos semanas* " (folio 244).
Por lo que se refiere a la alegación de que "*No existen ficheros de las grabaciones dado que no se realiza un almacenamiento y clasificación de las imágenes"* hay que significar que la mera secuencia cronológica de las grabaciones supone en sí misma un almacenamiento clasificado pues resulta obvio que, en caso de necesidad, ante cualquier acontecimiento vandálico o de otra índole, las imágenes podrían ser recuperadas y aportadas a la Policía como prueba, sin necesidad de otra organización más sofisticada de las imágenes captadas. Por lo tanto, dichas alegaciones deben ser desestimadas.

VI

El artículo 44.3.a) de la LOPD tipifica de infracción grave:
"*Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general publicada en el Boletín Oficial del estado o Diario oficial correspondiente"*.
El IES "EL PLA" ha incurrido en la infracción descrita, al haber procedido a crear un fichero de titularidad pública, ya comenzó a recoger datos de carácter personal desde marzo de 2009, sin que, hasta la fecha, haya procedido a la inscripción en el Registro General de Protección de Datos.

VII

En conclusión, en el presente caso consta acreditada la existencia de varias cámaras interiores y exteriores, alguna de ellas orientada hacia la vía pública. Sin embargo no se ha podido constatar que tales cámaras capten imágenes ni del interior del Centro educativo ni de la vía pública que superen el principio de proporcionalidad establecido en la Instrucción 1/2006, que exige la ponderación en cada caso entre la finalidad pretendida y la posible afectación de las videocámaras al derecho al honor, a la propia imagen y a la intimidad de las personas y requiere, por tanto, la existencia de un razonable riesgo para la seguridad ciudadana. A este respecto hay que señalar que el sistema se instaló como medida disuasoria y para prevenir situaciones que se venían produciendo con regularidad como *"actos vandálicos, robos, destrozos de mobiliario del Centro y el inmueble, extorsiones y amenazas entre alumnos, menudeo y consumo de estupefacientes, agresiones, peleas y acoso escolar, destrozos de los sistemas de seguridad anti-incendios (rotura de extintores, mangueras y puerta cortafuegos)"*
Por tanto, de acuerdo con los principios señalados procede el archivo las presentes actuaciones respecto de la infracción del artículo 6 imputada.
Por lo que respecta a la infracción imputada del artículo 20, ha quedado acreditado que, desde el 3 de marzo de 2009, fecha en que el sistema de videovigilancia del IES "EL PLA" entró en funcionamiento, dicho IES utilizó el fichero de datos de carácter personal *"FICHERO DE VÍDEO VIGILANCIA"* sin que, hasta la fecha, dicho fichero haya sido inscrito en el Registro General de Protección de Datos.
Por lo tanto, está acreditado que el IES "EL PLA" creó un fichero de titularidad pública y procedió a iniciar la recogida de datos de carácter personal con anterioridad a la inscripción en el Registro General de Protección de Datos, conducta que supone la vulneración del artículo 20 de la LOPD.
Vistos los preceptos citados y demás de general aplicación, El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: Declarar el **ARCHIVO** de las presentes actuaciones respecto de la infracción imputada del artículo 6 de la Ley Orgánica 15/1999..

SEGUNDO: Declarar que el **INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA"**, ha infringido lo dispuesto en el artículo 20 de la LOPD, tipificada como grave en el artículo 44.3.a) de la Ley Orgánica 15/1999.

TERCERO: REQUERIR al **INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA",** para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 20 de la LOPD y, en concreto, que proceda a la inscripción del fichero de *"VIDEOVIGILANCIA*" en el Registro General de Protección de Datos.
Las resoluciones que recaigan en relación con las medidas y actuaciones adoptadas, deberán ser comunicadas a esta Agencia Española de Protección de Datos, de acuerdo con el artículo 46.3 de la LOPD. La citada comunicación deberá realizarse en el plazo de un mes.

CUARTO: NOTIFICAR la presente resolución y el Anexo 1 al **INSTITUTO DE ENSEÑANZA SECUNDARIA "EL PLA"** y al superior jerárquico la ***CONSELLERÍA DE EDUCACIÓN DE LA GENERALITAT VALENCIANA*** y a **cada uno de los denunciantes** el presente Acuerdo y exclusivamente el Anexo que les corresponda, en el que se incluye su identificación, de conformidad con lo estipulado en el artículo 13.2 del REPEPOS.

QUINTO: 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 Contenciosoadministrativo 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.

Madrid, 12 de abril de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Expediente Nº: E/00701/2009

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES
De las actuaciones practicadas por la Agencia Española de Protección de Datos ante **CENTROS DE ENSEÑANZA ALMAZAN, S.A.** en virtud de denuncia presentada ante la misma por **D. A.A.A.**y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 15 de enero de 2009, tuvo entrada en esta Agencia un escrito de en el que se denuncia la instalación de cámaras de videovigilancia en **COLEGIO EUROPEO ALMAZÁN**.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, lo que se verificó requiriendo al titular del establecimiento denunciado para que acreditara que el sistema de videovigilancia instalado cumple con los requisitos exigidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
En concreto, se solicitó la acreditación de los siguientes extremos: - Identificación de la entidad responsable (Nombre completo o razón social y NIF o CIF) - Detalle de los lugares donde se encuentran ubicadas las cámaras de videovigilancia. - Especificar claramente la finalidad por la cual se han instalado las mismas. - Información sobre la existencia de monitores en el local que permitan visualizar las imágenes captadas por las videocámaras. - Copia del cartel o carteles donde se informa de la existencia de cámaras de videovigilancia e indicar la ubicación de los mismos. Además, adjuntar modelo del formulario informativo que debe estar a disposición de los ciudadanos según se recoge en el artículo 3.b de la Instrucción 1/2006 e informar del procedimiento establecido para distribuir los formularios ante una petición del mismo. - Identificación de la empresa de seguridad que ha realizado la instalación de las videocámaras y copia del contrato de prestación de servicios firmado con la misma. - Copia de la documentación acreditativa de que la empresa de seguridad está autorizada por el órgano administrativo competente del Ministerio del Interior como empresa de seguridad privada. - Copia de documentación que permita comprobar que la empresa de seguridad ha notificado las características de la citada instalación a la autoridad competente en materia de seguridad privada. - Copia de la autorización administrativa emitida por la autoridad gubernativa correspondiente, según prevé el Reglamento de Seguridad Privada, para realizar la instalación de las cámaras de videovigilancia en el exterior. - Detalle de las personas que pueden acceder al sistema de videovigilancia instalado, indicando si las imágenes son únicamente visualizadas o también se graban. - Si las imágenes se graban, describir el sistema utilizado, quién accede al mismo y detallar el tiempo de conservación de las mismas. En este caso además, adjuntar el código de inscripción del fichero en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o en su defecto, solicitud de inscripción del fichero en el citado Registro.
De la información aportada por el denunciado, se pone de manifiesto lo siguiente:
· La entidad responsable es “CENTROS DE ENSEÑANZA ALMAZÁN S.A.”. · Presentan un documento en el que explican la ubicación de las cámaras.· La finalidad es la seguridad del edificio y sus ocupantes, evitando la repetición de los altercados

acontecidos en las inmediaciones del colegio. · Existe un monitor de 17“ para la visualización de las imágenes. · Adjunta copia del cartel informativo de la existencia de las cámaras de videovigilancia. · La instalación fue realizada por la empresa “ABYMATIC SISTEMAS, S.L.”, debidamente autorizada por el Ministerio del Interior. Asimismo adjunta copia del contrato de prestación de servicios.
· Adjunta autorización de la mencionada empresa por el Ministerio del Interior. · Manifiesta que la instalación ha sido notificada a la autoridad competente. · Solo puede acceder al sistema y visualizar las imágenes captadas Dña B.B.B.. Las obligaciones de confidencialidad y secreto de la empleada están registradas en el documento de confidencialidad firmado al efecto y del que se aporta copia. · El tiempo máximo de grabación de imágenes es de 20 días, borrándose las grabaciones superiores a dicho plazo automáticamente. · Adjuntan solicitud de inscripción del fichero en el Registro General de Protección de Datos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 6 de la LOPD exige el consentimiento de los afectados para el tratamiento de sus datos personales salvo que la Ley determine otra cosa o cuando concurra alguna de las circunstancias previstas en el apartado 2 del citado artículo 6. En el caso que nos ocupa, la habilitación legal para el tratamiento de las imágenes de las personas físicas con fines de vigilancia procede de la Ley 23/1992, de 30 de junio, de Seguridad Privada existiendo, únicamente, legitimación para dicho tratamiento si la instalación y/o el mantenimiento del sistema de vigilancia se realiza por una empresa de seguridad autorizada por el Ministerio del Interior.
La Ley 23/1992, de 30 de junio, de Seguridad Privada habilita a las personas físicas jurídicas privadas, que reúnan los requisitos previstos en su artículo 7, para la prestación de servicios de vigilancia y seguridad de personas o bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de seguridad pública.
El artículo 5 de la citada Ley enumera las posibles medidas de seguridad que podrán ser adoptadas, entre ellas la “*instalación y mantenimiento de aparatos, dispositivos y sistemas de seguridad*” y “*Explotación de centrales para la recepción, verificación y transmisión de las señales de alarmas y su comunicación a las Fuerzas y Cuerpos de Seguridad, así como prestación de servicios de respuesta cuya realización no sea de la competencia de dichas Fuerzas y Cuerpos*”.
Por otro lado, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, en cuyo artículo 3 se especifica lo siguiente: *“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:*
a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información

prevista en el artículo 5.1 de la Ley Orgánica 15/1999. El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de la Instrucción".
Por su parte, el artículo 6 de la citada Instrucción señala que "*los datos serán cancelados en el plazo máximo de un mes desde su captación*".
Finalmente indica dicha Instrucción en su artículo 7 lo siguiente: *"1 La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de protección de Datos, para su inscripción en el Registro General de la misma...*
2. A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real"

III

En supuesto presente, del examen de la documentación aportada por el titular del establecimiento denunciado se constata que el sistema de videovigilancia instalado en su establecimiento reúne los requisitos anteriormente descritos, por lo que no se aprecia la existencia de infracción a la LOPD
Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **CENTROS DE ENSEÑANZA ALMAZAN, S.A**. y a **D. A.A.A..** De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.
Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Expediente Nº: E/00729/2008

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante **ANPE-TENERIFE, CC OO ENSEÑANZA TENERIFE, CSI-CSIF CANARIAS, INSUCAN, OCESP** (Organización Canaria de Empleados y Servicios Públicos), y **SEPCA**, en virtud de denuncia presentada ante la misma por **DON P.P.P.,** y **DON A.A.A.,** en base a los siguientes,

HECHOS

PRIMERO: Con fechas de 7 de febrero y 16 de junio de 2008, tienen entrada en esta Agencia sendos escritos remitidos por Don P.P.P. y Don A.A.A., en los que exponen lo siguiente:

- Los sindicatos de la enseñanza de Canarias ANPE, CSI-CSIF, CC.OO., INSUCAN, OCESP y SEPCA han utilizado datos personales que posee la Consejería de Educación del Gobierno de Canarias, y han elaborado un documento en el que informan de una propuesta de referéndum sobre complementos retributivos, con datos de su vida profesional, entre los que figuran el destino docente, cuerpo al que pertenecen, situación laboral, años que les faltan para la jubilación y años de servicio a 1 de enero de 2008.
- Dichos documentos no se han entregado en persona, sino que se han dejado sobre una mesa en las salas de profesores, sin estar en sobres cerrados, por lo que cualquier profesor podía ver estos datos personales de otros profesores.

Los denunciantes aportaron copia de sendas cartas.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

- Con fecha 21 de mayo de 2008, se solicitó al Sr. P.P.P. información relativa a la fecha y lugar concreto en que encontró el documento a que hace referencia en su denuncia. No se ha recibido respuesta por su parte.
- Con fecha 29 de junio de 2008, se solicitó a los sindicatos ANPE, CSI-CSIF, CC.OO., INSUCAN, OCESP y SEPCA diversa información en relación con los hechos denunciados.
- Unión Provincial de Tenerife del sindicato CSI-CSIF, indicó que el Sr. P.P.P. no es afiliado a su central sindical, por lo que no consta en su base de datos, y que CSI-CSIF no emitió dichos documentos, sino que en todo caso lo hubiese hecho la plataforma sindical que se constituyó con ocasión de un referéndum, que implicaba a todo el personal docente de Canarias.
- La Federación de Enseñanza de CC.OO. de Canarias, expuso que los datos que constan en la base de datos de su sindicato, "…en el marco de la Negociación Colectiva llevada a cabo entre la Consejería de Educación, Universidades, Cultura y Deportes y este Sindicato y otros (ANPE, CSIF, INSUCAN, OCESP y SEPCA)" relativos a D. P.P.P. son su nombre y apellidos, DNI, fecha de nacimiento, antigüedad en el puesto de trabajo, Número de Registro Personal y localidad donde presta sus servicios como funcionario. El origen de los datos del Sr. P.P.P. que obran en su poder es el censo que la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias facilitó a cada uno de los sindicatos más representativos de cada unidad electoral en el marco de las Elecciones Sindicales celebradas en el año 2006, en la Inspección Educativa de Tenerife, Unidad Electoral de Santa Cruz de Tenerife. Esta información fue remitida a ese sindicato en aplicación de la normativa

relativa a las elecciones sindicales, en virtud del art. 67.1. del R.D. Legislativo 1/1995, por el que se aprueba el Texto Refundido del Estatuto de los Trabajadores. La entidad aporta copia de un listado correspondiente al censo electoral para las Elecciones Sindicales del año 2006, donde constan los datos de nombre, apellidos, DNI,. antigüedad y fecha de nacimiento del Sr. P.P.P.. En el marco de la negociación colectiva que se llevó a cabo entre los sindicatos más representativos en el sector de la Educación Pública en Canarias y el Gobierno de Canarias, la Comisión Negociadora del Convenio hizo entrega del documento al que alude el denunciante, en sobre abierto, pero entregado en mano al afectado. La entidad aporta copia del Preacuerdo firmado el 17/12/2007 entre la Consejería de Educación del Gobierno de Canarias y las centrales sindicales representativas del sector, ANPE, CSI-CSIF, CC.OO., INSUCAN, COESP y SEPCA. La Ley Orgánica 11/1985 de Libertad Sindical establece que "*… Los trabajadores afiliados a un sindicato podrán … recibir la información que le remita su sindicato.*".

- La Sección Sindical de Docentes de OCESP, realizó diferentes declaraciones, todas ellas en el mismo sentido que las manifestadas por CC.OO., detalladas anteriormente.
- El sindicato ANPE en Canarias, realizó las mismas manifestaciones que CC.OO. y OCESP. Aporta una carta firmada por el Sr. P.P.P., uno de los denunciantes, en la cual comunicaba que cedía sus datos personales al sindicato ANPE a efectos de que le pudiese informar sobre cuestiones laborales que pudiesen ser de su interés.
- El sindicato SEPCA, expuso que el Sr. P.P.P. no es afiliado a su organización, no figurando ningún dato suyo en el fichero de afiliados. A pesar de que en el documento aportado por los denunciantes aparecen las siglas de SEPCA, esta organización no elaboró ni participó en el tratamiento de datos que dio origen a dicho documento. Dicha comunicación se enmarca en el ámbito de una consulta a los trabajadores, amparada en el derecho fundamental a la libertad sindical (art. 68.1 de la Constitución Española, art. 8 de la Ley Orgánica 11/1985 de Libertad Sindical y art. 68.d de la Ley del Estatuto de los Trabajadores). Los datos que figuran en dicha carta personalizada parecen ser el resultado de un tratamiento de datos del censo electoral, proporcionado presumiblemente por la Consejería de Educación. Desconocen las circunstancias específicas de la elaboración de las cartas personalizadas, al no participar en su elaboración. Pero de la información disponible, consideran clara la voluntad del remitente al utilizar un sobre para su envío, que indica que la información que contiene era solo para la persona a quien iba dirigida.
- El escrito de solicitud de información dirigido al sindicato INSUCAN no fue recogido por dicho sindicato, siendo devuelto por el servicio de Correos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

Los hechos denunciados se concretan en el tratamiento de los datos personales realizados por varios sindicatos (años de servicio, años que restan para la jubilación) para elaborar una información acerca de la negociación colectiva referida a un nuevo marco retributivo de los docentes, y además está información se dejo en un sobre abierto sobre una mesa, pudiendo haber sido visto por cualquier compañero.

A este respecto, referido a todo tipo de datos personales, conviene señalar lo dispuesto en el artículo 6.1 y 2 de la LOPD, que consagra el principio de consentimiento:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

El artículo 3.c) de la citada LOPD define el tratamiento de datos como *"Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

El tratamiento de datos sin consentimiento de los afectados constituye, por tanto, un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F.J. 7 primer párrafo), *"... consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporciona a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)".*

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

El artículo 2.1 de la Ley Orgánica de Libertad Sindical 1/1985 (en lo sucesivo LOLS), señala que la libertad sindical comprende "*d) el derecho a la actividad sindical*."

El artículo 8 de la LOLS señala:

"1. Los trabajadores afiliados a un sindicato podrán, en el ámbito de la empresa o centro de trabajo:

a. Constituir secciones sindicales de conformidad con lo establecido en los estatutos del sindicato.

b. Celebrar reuniones, previa notificación al empresario, recaudar cuotas y distribuir información sindical, fuera de las horas de trabajo y sin perturbar la actividad normal de la empresa.

c. Recibir la información que le remita su sindicato.

2. Sin perjuicio de lo que se establezca mediante convenio colectivo, las secciones sindicales de los sindicatos más representativos y ***de los que tengan representación en los comités de empresa*** *y en los órganos de representación que se establezcan en las Administraciones Públicas o cuenten con delegados de personal, tendrán los siguientes derechos:*

a. Con la finalidad de facilitar la difusión de aquellos avisos ***que puedan interesar a los afiliados al sindicato y a los trabajadores en general****, la empresa pondrá a su disposición un tablón de anuncios que deberá situarse en el centro de trabajo y en lugar donde se garantice un adecuado acceso al mismo de los trabajadores.*
b. A la negociación colectiva, en los términos establecidos en su legislación."
Por último, el artículo 87.1 y 2 del Real Decreto Legislativo 1/1995, de 24 de marzo, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, establece:
Estarán legitimados para negociar:
1. En los convenios de empresa o ámbito inferior: el comité de empresa, delegados de personal, en su caso, o las representaciones sindicales si las hubiere.
En los convenios que afecten a la totalidad de los trabajadores de la empresa será necesario que tales representaciones sindicales, en su conjunto, sumen la mayoría de los miembros del comité. En los demás convenios será necesario que los trabajadores incluidos en su ámbito hubiesen adoptado un acuerdo expreso, con los requisitos del artículo 80 de esta Ley, de designación, a efectos de negociación, de las representaciones sindicales con implantación en tal ámbito.
En todos los casos será necesario que ambas partes se reconozcan como interlocutores.
2. En los convenios de ámbito superior a los anteriores:
a. Los sindicatos que tengan la consideración de más representativos a nivel estatal, así como, en sus respectivos ámbitos, los entes sindicales afiliados, federados o confederados a los mismos.
b. Los sindicatos que tengan la consideración de más representativos a nivel de Comunidad Autónoma respecto de los convenios que no trasciendan de dicho ámbito territorial, así como, y en sus respectivos ámbitos, los entes sindicales afiliados, federados o confederados a los mismos.
c. Los sindicatos que cuenten con un mínimo del 10% de los miembros de los comités de empresa o delegados de personal en el ámbito geográfico y funcional al que se refiera el convenio.
Indican los Sindicatos que han contestado a la solicitud de información de esta Agencia, que el día 17 de diciembre de 2007, se firmó un preacuerdo, en el marco de la Negociación Colectiva, entre algunas centrales sindicales y la Consejería de Educación, Universidades, Cultura y Deportes del Gobierno de Canarias, sobre un nuevo marco retributivo del personal docente no universitario de Canarias en el que se condicionaba la elevación del mismo a acuerdo sólo si era ratificado en referéndum dicho preacuerdo. El referéndum se celebró el día 30 de enero de 2008, por lo que la campaña informativa al personal docente se desarrolló durante el mes de enero. Con la finalidad de dar a los electores la mayor y mejor información de cuál sería su situación económica de aprobarse definitivamente el preacuerdo, se procedió a la elaboración de la carta personalizada, en la que se indicaban los años que faltaban para cumplir los 65 años y los años de servicios prestados a fecha 1 de enero de 2008. La carta se entregó e mano a cada destinatario, en sobre abierto.
Si bien el derecho a la libertad sindical se encuentra legalmente limitado por el ejercicio legitimo de los demás derechos fundamentales y la protección de bienes de relevancia constitucional, y a pesar del tenor literal de que el artículo 28.1 de la Constitución Española pudiera inducir a considerar la restricción del contenido de la libertad sindical a una vertiente exclusivamente organizativa, sin embargo en este precepto se integra también la vertiente funcional del derecho, es decir, el derecho de los sindicatos a ejercer aquellas actividades dirigidas a la defensa, protección y promoción de los intereses de los trabajadores, en suma a desplegar los medios de acción necesarios para que puedan cumplir las funciones que constitucionalmente les corresponde.

En el presente supuesto, se difunde en el ámbito de los trabajadores del colectivo de docentes información sobre ciertas cuestiones relacionadas con un nuevo marco retributivo que tendrá que ratificarse mediante referéndum, pudiendo entrar ésta dentro del derecho de libertad sindical.
La sentencia de la Audiencia Nacional de 19 de diciembre de 2007 manifiesta respecto de esta cuestión que "*el derecho a la libertad sindical, (…) ha de prevalecer sobre el derecho a la protección de datos personales, cuando, como sucede en el caso examinado, la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical*".
Asimismo, denuncian que los sobres conteniendo la información sobre los años de servicios prestados y el número de años que quedan para la jubilación se dejaron en un sobre abierto en la sala de profesores. En este sentido, hay que señalar que los Sindicatos afectados han indicado que se entregaron en mano a los profesores, cumpliendo con ello las cautelas establecidas en la normativa de seguridad. Por otro lado, dado que los sobres iban dirigidos a cada persona afectada, el abrirlo por persona distinta supondría una infracción al secreto de las comunicaciones postales.
Teniendo en cuenta lo expuesto, se considera que no ha existido vulneración de ningún precepto de la LOPD, por lo que procede acordar el archivo de las actuaciones.
Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a **ANPE-TENERIFE**, con domicilio en (C/……), **CC OO ENSEÑANZA TENERIFE**, con domicilio en (C/……), **CSI-CSIF CANARIAS**, con domicilio en (C/……), **INSUCAN**, con domicilio en (C/……), **OCESP (Organización Canaria de Empleados y Servicios Públicos)**, con domicilio en (C/……), **SEPCA** con domicilio en (C/……), y a **DON P.P.P.**, con domicilio en (C/……), **DON A.A.A.,** con domicilio en (C/……..).
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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio,

reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Expediente Nº: E/00956/2006

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CENTRO DOCENTE PRIVADO HIGHLANDS**, en virtud de denuncia presentada ante la misma por **D. F.S.F.**, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 24/07/2006, tuvo entrada en esta Agencia un escrito de D. F.S.F.(en lo sucesivo el denunciante), en el que denuncia que como parte del proceso de admisión realizado por su hija para el ingreso en el Centro Docente Privado Highlands (en lo sucesivo el Colegio), ésta fue sometida a un conjunto de "*pruebas escritas de nivel educativo y en tests psicológicos y de la personalidad, también por escrito*". Toda vez que no fue admitida y al solicitar explicación detallada del porqué de tal decisión, señala que "*el centro, se negó y se sigue negando a dar los criterios de valoración [...] incumpliendo clamorosamente el artículo 13.3 de la Ley de Protección de Datos de Carácter Personal*". Manifiesta, además, que "*cuando hemos solicitado que dado que ya no los necesitan, se nos entreguen las pruebas y cuantos documentos escritos haya realizado la menor, cancelando la totalidad de los datos con que cuenten, el centro se niega contumazmente a entregárnoslo*".

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados.

TERCERO: Dentro de las actuaciones previas de investigación, se realizó una visita de inspección al Colegio el 25/11/2006, con el siguiente resultado:

1. El Colegio mantiene para los fines derivados de su gestión el fichero automatizado denominado "AMIC", que figura inscrito en el Registro General de Protección de Datos con código ######## bajo la descripción *"Gestión Académica, Administrativa, Personal, Alumnos, Padres de Familia".* Está registrado como de nivel *"alto"* en lo referido al establecimiento de las medidas de seguridad definidas en la legislación sobre Protección de Datos.
2. El Colegio ofrece enseñanza en los niveles de Educación Infantil, Primaria, Secundaria y Bachillerato, con el carácter de privado, estando autorizado por la Junta de Andalucía para impartir Enseñanzas de Régimen General con el código #########.
3. El procedimiento de admisión de alumnos en el Colegio incluye la solicitud a los padres a fin de que cumplimenten un formulario denominado *"PRE-SOLICITUD DE INGRESO"* mediante el cual se recaban datos de carácter personal de los padres y del menor para el que se solicita plaza, siendo el único documento que firman los padres o los representantes legales de los niños durante el proceso de admisión. Dicho documento incorpora una cláusula de información del siguiente tenor:

"*De acuerdo con la normativa vigente en materia de Protección de Datos de Carácter Personal le informamos y Ud. presta su consentimiento para la incorporación de sus datos personales y de correo electrónico, a los ficheros automatizados existentes en el colegio Highlands, y al tratamiento automatizado al que van a ser sometidos los mismos con la finalidad de proporcionarle nuestros servicios y el envío de publicidad y ofertas del Colegio u otras entidades relacionadas con el Colegio. Tiene derecho de acceso, rectificación y cancelación que podrá ejercitar por carta a nuestro domicilio en la (C/.....). Ud. acepta que sus datos puedan ser cedidos*

exclusivamente para las finalidades a las que se refiere esta cláusula, a otras entidades o asociaciones relacionadas con el Colegio".
Posteriormente, se realiza una entrevista con el Director del Colegio o alguno de sus asistentes, en la que se trata de evaluar la idoneidad de la familia de acuerdo a los criterios que dimanan de su ideario educativo. Respecto al niño, se le realizan un conjunto de pruebas de índole psicotécnica o de evaluación de conocimientos – que pueden variar en función de la edad – a fin de verificar si reúne las características exigidas por el Colegio para la admisión. Finalmente, reunido el Consejo Escolar, se toma una decisión sobre las solicitudes, que es comunicada de forma personal a cada una de las familias, realizándose por correo postal certificado a las familias cuyas solicitudes de admisión no han sido aceptadas.
4. Toda la documentación generada durante el proceso de admisión es destruida por el Colegio, no conservándose ningún reflejo de las solicitudes en el fichero del Centro. En el caso de los alumnos aceptados, se inicia el proceso de matriculación volviendo a recabar todo el conjunto de datos de carácter personal necesarios.
5. Respecto a las solicitudes realizadas con fechas 21 y 26/06/2006 por el denunciante ante el Colegio solicitando "*la totalidad de la documentación escrita de la totalidad de las pruebas que su hija realizó en su centro escolar*" y "*los criterios de valoración y las conclusiones de las pruebas que hayan servido para adoptar dicha decisión*", y en la que se manifestaba que "*no cuentan con autorización de los padres para conservar por más tiempo ni los datos ni el soporte de dichos datos*", el Colegio contestó mediante escrito, de 01/09/2006, en el que hacía constar lo siguiente:
• "*Que los criterios de selección del alumnado del Colegio Highlands corresponden al ámbito de autonomía administrativa y de organización [...] como colegio privado que es, [...] y que se realizan en todo caso, con respeto a los valores, principios y derechos constitucionales*".
• "*Que toda la información recabada en el proceso de admisión [...] fue destruida íntegramente una vez concluido dicho proceso de admisión, no constando dato alguno de la misma en los archivos del Colegio ni de la Congregación Religiosa titular del mismo*".
6. Realizada comprobaciones por parte de los inspectores en el fichero automatizado del Colegio así como en los ficheros en papel custodiados en la Secretaría del Centro y en el despacho de la "Cargo 1 " del mismo, no pudo verificarse la presencia, en el momento de la inspección, de documentación con datos de carácter personal o registros en ficheros a nombre de la menor en cuestión o de sus progenitores.
7. En los ficheros de expedientes en papel, no se encontró información relativa al proceso de admisión en los expedientes de los alumnos del Colegio.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 6.1 de la LOPD dispone lo siguiente:
"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."

Del escrito presentado ante esta Agencia por el denunciante se desprende claramente que dio su consentimiento para que el Colegio realizara el tratamiento de los datos personales su hija, menor de edad, con la finalidad de que fuera admitida como alumna en dicho Colegio.

III

El artículo 4.5 de la LOPD dispone lo siguiente:
"5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos."
Asimismo, el artículo 16de la citada Ley Orgánica señala en su punto 5:
"5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado."
De la inspección realizada al Colegio por los servicios de Inspección de esta Agencia, ha quedado acreditado que no figura dato personal alguno de la menor ni de sus progenitores en los ficheros informáticos o tipo papel del Colegio. Por otra parte, el resultado de la inspección concuerda con el escrito emitido por el Colegio, en el sentido de que todos los datos recabados durante el proceso de admisión habían sido destruidos una vez concluido dicho proceso, por lo que no constaban datos de la menor en sus archivos. Por tanto, el
Colegio actuó de acuerdo a la normativa de protección de datos citada cuando, al finalizar el proceso de admisión por no existir relación contractual con el denunciante, canceló los datos obtenidos con el consentimiento del denunciante, dado que ya no eran pertinentes para la finalidad para la que fueron recabados, puesto que no se admitió a la hija del denunciante como alumna del citado Colegio privado.
Así pues, aunque el artículo 13 de la LOPD recoge que "…*el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.",* en el presente caso, al haber cancelado el Colegio los datos obtenidos de la hija del denunciante cuando dejó de existir la finalidad para la que fueron recabados, de acuerdo a la normativa de protección de datos, no pudo atender la petición del denunciante, sin que por ello pueda apreciarse que haya vulnerado la LOPD. Por tanto, procedería el archivo de las actuaciones.
Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **CENTRO DOCENTE PRIVADO HIGHLANDS, (C/.....)** y a **D. F.S.F. (C/.....)**.

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.
Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción
Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Expediente Nº: E/01047/2007

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad **CENTRO LIBER FORMACIÓN, S.L., FOREM (FUNDACIÓN Y EMPLEO MIGUEL ESCALERA)** en virtud de denuncia presentada ante la misma por **DÑA.MAR CIORRAGA SOUTO** y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 11 de abril de 2007, tuvo entrada en esta Agencia escrito de D./Dña.C.C.C. CENTRO LIBER FORMACIÓN, S.L., FOREM (FUNDACIÓN Y EMPLEO MIGUEL ESCALERA) el/la denunciado/a) en el que denuncia
Con fecha de 11/4/2007 tiene entrada en esta Agencia un escrito de Dña.C.C.C. (en lo sucesivo la denunciante),en el que manifiesta que es representante legal de MARCIO DISEÑO, SL, cuyo objeto social es la enseñanza para adultos y utiliza la marca comercial GOYMAR.
En septiembre de 2005, CENTRO LIBER FORMACIÓN, SL, (en lo sucesivo LIBERFORMACIÓN), contrató a GOYMAR el alquiler de un aula propiedad de ésta última para la impartición de 2 cursos de "Diseño asistido por ordenador II". Se aporta contratos de arrendamiento del aula. Los cursos estaban subvencionados por la Comisión Tripartita FOREM, fundación de carácter privado promovida por la Confederación Sindical de CCOO.
LIBERFORMACIÓN encargó a GOYMAR la captación de alumnos, contratación de profesores y alquiler de espacios docentes, por lo que GOYMAR recabó datos personales de los alumnos y profesores con los que contactó mediante la solicitud de participación **cuyo modelo adjuntan**.
En febrero de 2006, ya acabados los cursos contratados en septiembre de 2005, LIBERFORMACIÓN propone a GOYMAR un nuevo curso de patronaje por ordenador, por lo que para la captación de alumnos se contactó con los de los cursos impartidos en septiembre de 2005 recibiendo de todos idéntica respuesta: que ya lo sabían pues una tal María les había informado diciéndoles que tenía todos sus datos al haber realizado en septiembre un curso en GOYMAR y les llamaba para informarles de un nuevo curso de patronaje por ordenador.
Puestos en contacto con LIBERFORMACIÓN, éstos dicen que sólo le han dado los datos a FOREM, resultando que la persona que efectuó las llamadas a los alumnos que anteriormente habían realizado el curso de septiembre de 2005 estuvo trabajando tiempo atrás en FOREM.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:
1. En los contratos de fecha 26/9/2005 suscritos entre CENTRO LIBER FORMACIÓN, SL, Y MARCIO DISEÑO, SL, (GOYMAR) en relación con el arrendamiento de dos aulas aportado por Dña.C.C.C. y por LIBERFORMACIÓN, no se menciona la entrega de datos personales y no contiene las especificaciones del artículo 12 de la LOPD.
2. La representante de LIBERFORMACIÓN, en su escrito con fecha de entrada de 1/2/2008 manifiesta que para garantizar que el número de alumnos es el establecido en los contratos de alquiler de las aulas y teniendo en cuenta que GOYMAR es un centro de formación, informó a sus alumnos acerca de la posibilidad de realizar los cursos objeto de la denuncia. Ante el interés mostrado por los alumnos, GOYMAR

pone en conocimiento de LIBERFORMACIÓN este hecho, comunicándole los datos de dichos alumnos.
Por otra parte, aunque LIBERFORMACIÓN es quien contrata a los profesores, los datos de éstos son igualmente facilitados a dicha entidad por GOYMAR. Los formularios oficiales de solicitud de participación son entregados por LIBERFORMACIÓN a GOYMAR.
Las entregas de datos de GOYMAR a LIBERFORMACIÓN se realizaron entre el 26 de septiembre de 2005 y el 20 de febrero de 2006 aproximadamente.
LIBERFORMACIÓN, tras recibir los datos previamente cedidos por GOYMAR, envía los datos a FOREM, en cumplimiento de los contratos de "ejecución de acciones formativas" establecido con FITEQA, cuya copia adjuntan y que contiene las especificaciones del artículo 12 de la LOPD. De dichos contratos se deduce que las únicas acciones que realiza LIBERFORMACIÓN sobre los datos personales de los alumnos, se concretan en el envío a FOREM de la información relativa a los mismos en cumplimiento de los citados contratos, sin que LIBERFORMACIÓN utilice los datos personales para finalidades propias.
En el escrito con fecha de entrada de 31/3/2008, se encuentran los datos remitidos por GOYMAR a LIBERFORMACIÓN y los enviados por ésta a FOREM. Las entregas se realizan entre el 26/09/2005 y el 20/02/2006.
Por otra parte, al tratarse de cursos solicitados por FITEQA, LIBERFORMACIÓN está obligada a proporcionar los datos de los participantes a dicha entidad, con la finalidad de que ésta pueda hacer un seguimiento del buen uso de la subvención otorgada. La entrega se realizó vía email en fechas anteriores al inicio del curso, según sus propias manifestaciones.
Según consta en el escrito con fecha de entrada de 31/3/2008, la carta de presentación del curso entregada a los participantes, tenían en su encabezado, anagramas de "*fiteqa – CC.OO*", "Fondo Social Europeo", "Fundación Tripartita" y "FOREM".
• Constan las copias de los siguientes contratos aportadas por LIBERFORMACIÓN:
- Contrato de 8/3/2005, suscrito entre Federación Estatal de Industrias Textil-Piel , Químicas y Afines de CC.OO. (FITEQA), y LIBERFORMACIÓN. Contiene las especificaciones del art. 12 de la LOPD.
- Contrato de 9/3/2005, suscrito entre Federación Estatal de Industrias Textil-Piel , Químicas y Afines de CC.OO. (FITEQA), y LIBERFORMACIÓN. No contiene las especificaciones del art. 12 de la LOPD.
- Contrato de 26/9/2005, suscrito entre LIBERFORMACIÓN y MARCIO DISEÑO, SL, (GOYMAR). No contiene las especificaciones del art. 12 de la LOPD.
3. Dña.C.C.C., denunciante y representante de MARCIO DISEÑO, SL, (GOYMAR), en su escrito de julio – 2008, manifiesta que se entregaron a LIBERFORMACIÓN a primeros de julio de 2008, los datos relativos a 30 alumnos y 2 profesores del curso "Diseño asistido por ordenador II", cuya relación nominal aporta.
4. En la solicitud de participación en el curso que debían cumplimentar los alumnos, y que se encuentra como DOC. 4 de la denuncia, se encuentra la siguiente información:
"Asimismo, y a los efectos de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa de desarrollo, autoriza la utilización de los datos personales contenidos en el presente documento y su tratamiento informático para la gestión de la solicitud a que se refiere el mismo. Y por el Servicio Público de Empleo a efectos de seguimiento, control y evaluación de la formación recibida."

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 6.1 y 2 de la LOPD, que consagra el principio de consentimiento:
"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

Por su parte, el artículo 11.1 y 2 de la LOPD dispone lo siguiente:
"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
a) Cuando la cesión está autorizada en una Ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.
c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".
La LOPD define, en su artículo 3.i), la *"cesión o comunicación de datos"* como *"toda revelación de datos realizada a una persona distinta del interesado"*, y el Real Decreto 1332/1994, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, considera cesión de datos *"toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada"*.
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 personales y a la libre circulación de estos datos, se refiere en su artículo 2.b) a la cesión, dentro de la definición del tratamiento de datos, y la define como *"comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso de los datos, cotejo o interconexión"*.

III

En el presente caso, se denuncia una presunta cesión de datos personales, sin embargo de los documentos aportados por la denunciante y de las actuaciones previas de investigación efectuadas por parte de la Subinspección de Datos de esta Agencia , no han quedado acreditado suficientemente los hechos denunciados.
En primer lugar, hay que señalar que la presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional en su Sentencia 76/1990 de 26 de abril considera que el derecho a la presunción de inocencia comporta: *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio."*
Conforme señala el Tribunal Supremo , en su Sentencia de fecha 26/10/98, el derecho a la presunción de inocencia *"no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsución estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo."*
El Tribunal Constitucional, en su Sentencia 24/1997, tiene establecido que *"los criterios para distinguir entre pruebas indiciarias capaces de desvirtuar la presunción de inocencia y las simples sospechas se apoyan en que:*
a) La prueba indiciaria ha de partir de hechos plenamente probados.
b) Los hechos constitutivos de delito deben deducirse de esos indicios (hechos completamente probados) a través de un proceso mental razonado y acorde con las reglas del criterio humano, explicitado en la sentencia condenatoria (SSTC 174/1985, 175/1985, 229/1988, 107/1989, 384/1993 y 206/1994, entre otras)."
En consecuencia, al no haber quedado suficientemente probados los hechos, denunciados de acuerdo a todo lo anteriormente expuesto, procedería el archivo de las actuaciones.
Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a **CENTRO LIBER FORMACIÓN, S.L**. con domicilio en (C/.....), y a **Dña.C.C.C.** con domicilio en (C/.....).

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 el artículo 116 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.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción

Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Expediente Nº: E/01533/2008

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la **UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA,** en virtud de denuncia presentada ante la misma por **DON M.M.M.**, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 10 de julio de 2008, tuvo entrada en esta Agencia escrito remitido por Don M.M.M., en el que denuncia a la Universidad Nacional de Educación a Distancia (UNED). Los hechos que pone de manifiesto son los siguientes:

- La Universidad Nacional de Educación a Distancia (UNED) facilita a sus alumnos el acceso al espacio virtual de la UNED, denominado CiberUNED. Entre los servicios telemáticos que para sus alumnos están disponibles en dicho espacio se encuentran los denominados Cursos Virtuales.

- Para acceder al servicio "Cursos Virtuales Alumnos" es necesario autenticarse en el sistema mediante un Identifícador de Usuario -que genera y nos asigna la propia UNED- junto con una Clave de Acceso, contraseña, asociada a dicho identifícador y que es personalizada o modifícable.

- Una vez autenticados en los Cursos Virtuales, los alumnos tenemos acceso al curso virtual de cada asignatura en la que estemos matriculados.

- El uso de las herramientas de comunicación, presentes en cada curso virtual, da acceso a las tutorías telemáticas en las que alumnos y profesores (miembros del equipo docente) interactuamos mediante el envío de mensajes a los foros temáticos habilitados. Con el envío de mensajes, tanto por parte de profesores como de alumnos, está contemplada la posibilidad de adjuntar ficheros.

Información de la UNED sobre cursos virtuales disponible en:

http://....X..../.....

https://...Y.../.....

- PSICOLOGÍA SOCIAL II es una asignatura anual que forma parte del Plan de Estudios (Plan 2000) conducente al título de Licenciado en Psicología por la UNED. Los alumnos matriculados en esta asignatura tenemos derecho de acceso al correspondiente curso virtual que el equipo docente de dicha asignatura gestiona. Los miembros del equipo docente utilizan los foros por ellos habilitados en la tutoría telemática para que, entre otras cosas, podamos descargar los ficheros por ellos adjuntados en los mensajes de su autoría.

- En fecha 27 de Junio de 2008, el equipo docente de la asignatura PSICOLOGÍA SOCIAL II ha publicado un mensaje en uno de los foros temáticos, de nombre "Principal, en el que se nos ha facilitado -a todos los alumnos de alta en dicho curso- la posibilidad de descargar un fichero, denominado "PARTICIPANTES_ACTIVIDADES.pdf\ que contiene un listado de alumnos en el que se ha pretendido detallar el nombre y apellidos de algunos alumnos junto con su DNI correspondiente. Mi nombre figura en dicho listado y aunque -por error en la confección del listado- no me corresponde el DNI asignado, mi DNI real está, aunque asignado a otro alumno/a. El objetivo de divulgar dicho fichero era, precisamente, que indicásemos al equipo docente si habíamos detectado en dicho listado algún error en la asociación de nuestros nombre/s y apellidos a nuestros DNI verdaderos.

En prueba de ello, véase ANEXO 1 y ANEXO 2.

- No me consta haber autorizado a que la UNED divulgue, a través de las tutorías telemáticas, listado alguno donde se relacione, o pretenda relacionarse, de manera inequívoca, mi n° de DNI asociado a mi nombre y ape llidos. Con este hecho, la UNED ha cedido datos de carácter personal dentro del ámbito de las tutorías telemáticas al

proporcionar los DNI adscritos a los concretos titulares de los mismos. Datos que, a partir de aquí, pueden divulgarse a otros ámbitos sin control por parte del cedente.
- La UNED impone a sus alumnos que salgan identificados con su nombre y apellidos, en lugar de identificarse con su Identificador de Usuario, cada vez que un alumno participa activamente en las tutorías telemáticas, poniendo mensajes en los respectivos foros de los cursos virtuales. Con esta práctica es muy posible averiguar, hoy día, el DNI correspondiente dado que en los Boletines Oficiales, accesibles desde cualquier conexión a Internet, podemos localizar el número del DNI asociado al nombre y apellidos de su titular. Sería deseable que nuestra participación activa en las tutorías telemáticas no exigiese difundir nombre y apellidos del autor de los mensajes.
- La UNED gestiona el teléfono de información automática (SIRA) ######## al que desde cualquier teléfono se puede llamar y simplemente indicando los dígitos de un DNI cualquier persona -alumno o no de la UNED- puede conocer las calificaciones del titular de dicho DNI. Les autorizo, a efectos de prueba, a que llamen al n° de teléfono arriba indicado y pronuncien o tecleen los dígitos de mi DNI; un sistema automático de voz les informará de las asignaturas a las que me presenté junto con las calificaciones obtenidas. En ningún momento se pide Clave de Acceso, o cualquier otra contraseña, para acceder a esta información de carácter personal. De esta manera, conociendo únicamente el DNI de un alumno podremos averiguar sus últimos resultados académicos en la carrera de psicología por la UNED. Actualmente, en ese n° de teléfono se informa tanto de las calificaciones de los exámenes realizados en la convocatoria de Junio 2008 como de la calificación final obtenida en cada asignatura. Desconozco hasta qué fecha estará disponible este servicio; actualmente lo está. Entiendo que no queda preservada la privacidad de las calificaciones cuando a éstas se pude acceder realizando una llamada telefónica e indicando únicamente el DNI del alumno a consultar. Se acompaña justificación de la existencia de estos teléfonos en el ANEXO 3.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:
1. En la documentación anexa facilitada por el denunciante figura un correo y la impresión del documento que figura anexo a ese correo. El correo ha sido emitido por el "*Equipo Docente*" en fecha de 27 de junio de 2008, figurando en el texto que el listado de participantes en las actividades voluntarias se adjunta con objeto de que los alumnos verifiquen que se encuentran registrados en la lista y que su DNI aparece correctamente. El listado en cuestión se compone de número de DNI y nombre y apellidos.
2. Con fecha 22 de enero de 2009 se recibió escrito de la "Cargo 2" Académica y Administrativa de la UNED en el que facilita diversa información con relación a la solicitud de información realizada por esta Agencia.
3. En su escrito manifiesta lo siguiente respecto a los motivos por los que a través de la herramienta de mensajería disponible en el curso virtual de la asignatura PSICOLOGÍA SOCIAL II, el Equipo Docente remitió el correo en el que se incluía el número de DNI de los alumnos:
La Universidad Nacional de Educación a Distancia es, junto con la UIMP, la única Universidad de ámbito estatal y se encuentra adscrita al Ministerio de Ciencia e Innovación a través de la Secretaría de Estado de Universidades.
El método de aprendizaje a distancia cuenta con un elemento esencial de apoyo a los estudiantes: los cursos virtuales.

En el caso de las enseñanzas regladas que imparte la UNED, los cursos virtuales se encuentran alojados en la plataforma Web-CT, que cuenta con las siguientes utilidades:
Material didáctico: Todo tipo de materiales adecuados para el seguimiento del curso.
Trabajos: Espacio donde se organizan los trabajos entregados por los alumnos para su posterior evaluación
Evaluación: Herramienta de evaluación.(exámenes)
Foros: herramienta de comunicación asíncrona entre los usuarios de un curso. Todos los mensajes son visualizados por todos los usuarios acreditados.
Correo: herramienta de comunicación asíncrona entre los usuarios de un curso. Los correos sólo son vistos por los destinatarios de los mismos. Herramienta equivalente al correo electrónico de una institución pero restringido a los usuarios de un curso
El Correo es, pues, una herramienta de comunicación personal en la que sólo el remitente y el destinatario o destinatarios de un mensaje pueden leer su contenido o acceder a los archivos adjuntos al mismo.
El Correo permite que el equipo docente y los alumnos intercambien mensajes entre sí; permite además guardar borradores de mensajes, buscar mensajes y añadir carpetas de correo.
Psicología Social II es una asignatura correspondiente a las enseñanzas regladas de Psicología, su curso virtual está alojado en la plataforma web-CT y cuenta con las herramientas anteriormente mencionadas, entre las que se encuentra el correo.
El equipo docente de la asignatura procedió a comunicar mediante la herramienta dispuesta al efecto, el listado de los alumnos que habían participado en las actividades voluntarias establecidas por el equipo docente y que serán objeto de valoración a los efectos de la calificación definitiva de los estudiantes.
La inclusión en el listado de estudiantes adjunto al correo del número de DNI corresponde a la necesidad de que éstos estén correctamente identificados, lo que se ha considerado que se trata de un acto que resulta necesario para la adecuada organización y seguimiento de su evaluación. Esta actuación se ha realizado al amparo de lo previsto en el apartado tercero de la disposición adicional vigésimo primera de la Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, que expresamente señala: "No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación."
4. Respecto de si el usuario de correo “EQUIPO DOCENTE”, que envió el correo en cuestión, pertenece a personal de esa Universidad y el detalle de cuáles son las funciones que desempeña manifiesta lo siguiente:
El usuario de la plataforma, y por tanto, de todas sus utilidades, entre ellas el correo "Equipo Docente" está formado por el personal docente e investigador de la UNED.
En el caso que nos ocupa, el usuario "Equipo Docente" está formado por el equipo docente de la asignatura "Psicología Social II".
De acuerdo con el artículo 180 de los Estatutos de la UNED, aprobado por el Real Decreto 426/2005, de 15 de abril, "Son deberes del profesorado, además de los establecidos en la legislación vigente:
a) Desempeñar adecuadamente las tareas docentes e investigadoras propias de su puesto de trabajo y régimen de dedicación, así como prestar la debida atención a sus alumnos, en especial dentro del horario establecido para ello.
b) Contribuir al buen funcionamiento de la universidad como servicio público, con especial atención al alumnado, y desarrollar sus funciones de acuerdo con los principios de legalidad y eficacia.

c) Elaborar los materiales didácticos de las asignaturas dentro de los plazos establecidos en cada caso para garantizar el correcto funcionamiento de la docencia.
d) Actualizar la formación para perfeccionar su actividad docente e investigadora.
e) Ejercer con responsabilidad los cargos para los que haya sido elegido o designado.
f) Participar en los procedimientos establecidos en la universidad para el control y la evaluación de su actividad docente y de investigación.
g) Aceptar los desplazamientos que les sean requeridos para atender las pruebas presenciales y las conferencias y encuentros con los alumnos en los centros, a instancias de éstos y de los profesores tutores. En el caso de ausencia por conferencias o encuentros, se garantizará siempre la debida atención al resto del alumnado.
h) Hacer un correcto uso de las instalaciones, bienes y recursos que forman el patrimonio de la universidad.
i) Informar anualmente por escrito de sus actividades docentes e investigadoras."
El desempeño de estas funciones es ejercido con arreglo a las normas internas que se establecen dentro de cada Departamento y con respeto al principio de libertad de cátedra, recogido en el artículo 178 de los mencionados Estatutos.
5. Respecto del sistema SIRA que permite conocer a los alumnos sus calificaciones académicas vía telefónica, aporta la siguiente información:

El Servicio de Información Automatizado de Calificaciones (SIRA) ofrece a los alumnos información de las calificaciones obtenidas en las enseñanzas regladas de la UNED por vía telefónica. El alumno dispone de un teléfono al que llamar, en el que se le solicita que teclee los dígitos completos del DNI y el sistema, automáticamente, le ofrece la información del resultado de sus calificaciones.
A los alumnos se les facilita información acerca del sistema SIRA en la página web de la UNED, motivo por el que considera que "*el acceso al sistema SIRA es voluntario para los alumnos y sólo podrán acceder a este servicio telefónico si, en el momento de realizar su matrícula, han autorizado expresamente que los datos de sus calificaciones sean incluidos en el SIRA".*
Aporta impresión de pantalla de la página de Internet del proceso de matriculación y del documento de matriculación, en el que se verifica que se solicita información al alumno acerca de si desea que sus datos personales sean incluidos en el Sistema Telefónico de Consulta de Calificaciones, denominación utilizada en la matriculación a través de Internet, o en el Servicio de Información Automatizado de Calificaciones, denominación utilizada en el documento de matriculación.
6. En el Registro General de Protección de Datos figura inscrito el fichero denominado "*GESTUVA*" con código número *#########*, descrito como "*gestión de cursos virtuales y registro de usuarios en los mismos*", cuyo responsable es la Universidad Nacional de Educación a Distancia.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

La denuncia se concreta en que la UNED ha facilitado los datos de nombre, apellidos y DNI del denunciante a todos los alumnos de la asignatura Psicología Social II.
El artículo 4.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), dispone que:
"*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.".*
Las "*finalidades*" a las que alude el apartado 2 ha de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley. Conforme a dicho precepto los datos sólo podrán tratarse cuando *"sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*
En consecuencia, si el tratamiento del dato ha de ser "*pertinente*" al fin perseguido y la finalidad ha de estar "*determinada*", difícilmente se puede encontrar un uso del dato para una finalidad "*distinta*" sin incurrir en la prohibición del artículo 4.2 aunque emplee el término "*incompatible*". A esta conclusión llega también el propio Tribunal Constitucional cuando en su Sentencia 292/2000 de 30 de noviembre establece: *" el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros...Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con éstos supone una nueva posesión y uso que requiere el consentimiento del interesado,"*
En definitiva, los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.
Por otro lado, el artículo 6.1 de la LOPD dispone que "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa."*
La UNED obtuvo lícitamente los datos de cada uno de los alumnos y con su consentimiento. La Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, en su disposición adicional vigésimo primera dispone:
"1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.
Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.
2. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido de los currículos a los que se refieren los artículos 57.2 y 62.3.
3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.
4. Igualmente no será preciso el consentimiento del personal de las universidades para la publicación de los resultados de los procesos de evaluación de su actividad docente, investigadora y de gestión realizados por la universidad o por las agencias o instituciones públicas de evaluación.
5. El Gobierno regulará, previo informe de la Agencia Española de Protección de Datos, el contenido académico y científico de los currículos de los profesores e investigadores que las universidades y las agencias o instituciones públicas de

evaluación académica y científica pueden hacer público, no siendo preciso en este caso el consentimiento previo de los profesores o investigadores.
Dado que la publicación de los listados de los alumnos matriculados en una asignatura puede considerarse como un acto necesario para el seguimiento de la evaluación o tutoría, no precisa del consentimiento de los afectados para su publicación. En consecuencia, no cabe deducir que se haya vulnerado el principio del consentimiento establecido en la LOPD, o que se hayan utilizado los datos para una finalidad incompatible con aquella para la que se obtuvieron.
Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a la **UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA** y a **DON M.M.M..**

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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de 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 citada 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.

Expediente Nº: E/01593/2009

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante las entidades APYMA DEL COLEGIO PUBLICO PATXI LARRAINZAR, ESCUELA PUBLICA PATXI LARRAINZAR, FEDERACIÓN SORTZEN-IKASBATUAZ, e INSTITUTO DE ESTADÍSTICA DE NAVARRA, en virtud de denuncia presentada ante la misma por DON ***A.A.A.,*** y en base a los siguientes

HECHOS

PRIMERO: Con fecha 14 de abril de 2009, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.***, en el que declara que, en marzo de 2009, recibió una carta, con membrete oficial del Gobierno de Navarra, a nombre de su hijo de dos años de edad. Denuncia la utilización de datos personales de niños de dos años sin el consentimiento de los padres por parte de la Escuela Publica Patxi Larrainzar de Pamplona.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. El denunciante aporta el sobre original de la carta que manifiesta haber recibido, y que va dirigida a ***B.B.B.***, calle (C/. …..C1). El sobre contiene un folleto en el que se informa de las ventajas de matricularse en el centro en la opción de Euskera. Aporta además copia del libro de familia en el que consta la fecha de nacimiento de ***B.B.B.***, en ***MES1 de 2006.

2. El día 1 de marzo de 2009 se realizó visita de inspección en las dependencias del colegio público Patxi Larrainzar, poniéndose de manifiesto los siguientes hechos:

a. La Directora del centro manifestó que la Asociación de Padres y Madres del Colegio (APYMA) colabora con el centro mediante campañas informativas, vía postal, en los periodos de prematriculación. Dichas campañas tienen como finalidad la difusión del modelo de enseñanza “D” (matriculación en la lengua euskera).

b. Para la realización de la campaña, el colegio facilitó a la APYMA sobres son el anagrama del colegio y una invitación a una reunión informativa, Estas campañas cuentan con la aprobación del Consejo Escolar del Colegio Patxi Larrainzar.

c. Desconoce el origen de los datos utilizados por la APYMA para el envío de las cartas informativas, ni del resto de los documentos informativos que ésta hubiera incluido además del referido anteriormente. d. ***B.B.B.*** no es, ni ha sido alumno del centro.

3. El día 1 de marzo de 2009 se realizó visita de inspección en las dependencias de la APYMA del colegio público Patxi Larrainzar, poniéndose de manifiesto los siguientes hechos:

a. La APYMA colabora con el colegio PATXI LARRAINZAR mediante campañas informativas, vía postal, en los periodos de prematriculación. Dichas campañas tienen como finalidad la difusión del modelo de enseñanza “D” (matriculación en la lengua euskera). Para la realización de la campaña, el colegio facilitó a la APYMA sobres son el anagrama del colegio y una invitación a una reunión informativa. La APYMA incluyó además un tríptico informativo sobre la matriculación en el modelo “D”. Los datos de los destinatarios de la campaña han sido facilitados por la Federación SORTZEN-IKASBATUAZ, de la cual la APYMA es miembro. Las etiquetas fueron elaboradas por algún miembro de la APYMA con sus propios medios, ya que la APYMA solo dispone de un ordenador inoperativo desde el año 2007.

b. La APYMA no conserva los listados facilitados por la Federación SORTZENIKASBATUAZ

4. El día 10 de marzo de 2009 se realizó visita de inspección en las dependencias de la Federación SORTZEN-IKASBATUAZ, poniéndose de manifiesto los siguientes hechos:

a. La Federación SORTZEN-IKASBATUAZ la componen Asociaciones de Padres y Madres de Alumnos de Colegios Públicos de Navarra (APIMAS) y algunos Centros Escolares, y también profesores. La APIMA del colegio Paxi Larrainzar es socio de pleno derecho de la Federación. La Federación tiene como objeto promover el modelo de enseñanza en euskera y una enseñanza de calidad.

b. El Presidente de la Federación SORTZEN-IKASBATUAZ manifestó que en cada curso escolar, cuando se inicia la campaña de matriculación en los centros públicos, la Federación solicita, mediante correo electrónico, al Instituto de Estadística del Gobierno de Navarra, el censo de los niños nacidos en el año al que corresponda la escolarización (niños de 3 años). Dicho censo es remitido por el Instituto de Estadística del Gobierno de Navarra mediante correo electrónico en formato de hoja de cálculo Excel. La dirección de correo electrónico a la que se remite la solicitud es la que consta en la página web del Instituto de Estadística de Navarra (estadistica@cfnavarra.es).

c. Posteriormente, la Federación facilita una copia de dicho censo a todas las Asociaciones de Padres y Madres de los colegios públicos que lo solicitan. Se les hace entrega en mano, bien en soporte CD-ROM o en PEN-DRIVE.

d. Una vez facilitado el censo a todas las Asociaciones que lo han solicitado se procede a la destrucción de todas las copias del mismo.

e. La Federación SORTZEN-IKASBATUAZ no conserva copia de datos remitidos por el INSTITUO DE ESTADISTICA NAVARRO, ya que han sido eliminadas todas las copias.

5. El día 10 de marzo de 2009 se giró visita de inspección en las dependencias del INSTITUTO DE ESTADISTICA DE NAVARRA, poniéndose de manifiesto los siguientes hechos:

a. El INSTITUTO DE ESTADISTICA DE NAVARRA recibe por distintas vías solicitudes de datos del padrón, siendo una de ellas a través de la dirección de correo electrónico estadistica@cfnavarra.es. Todas las solicitudes se analizan y solo en el caso que legalmente esté permitido, se facilitan los datos solicitados.

b. Cada año, cuando se inicia el periodo de matriculación de enseñanza oficial, se reciben peticiones de colegios públicos de Navarra de los datos de los niños que inician la enseñanza oficial (3 años). Por este motivo y al respecto, El INSTITUTO DE ESTADISTICA DE NAVARRA solicitó un informe jurídico, cuya copia ya ha sido aportada a la Inspección de Datos, entendiendo que se encuentra habilitado para facilitar los datos solicitados por los colegios públicos.

c. Los datos son facilitados a través de correo electrónico a la dirección facilitada por el colegio solicitante, en formato de hoja de cálculo EXCEL.

d. No le consta haber recibido peticiones de datos del censo por la Federación SORTZEN-IKASBATUAZ, ni haber facilitado a la misma datos personales.

e. El representante del INSTITUTO DE ESTADISTICA DE NAVARRA manifiesta que en dicho buzón estadistica@cfnavarra.es no se conservan las peticiones, pero se imprimen y se conservan en formato papel.

f. Se ha verificado que las solicitudes de peticiones de datos recibidas en el año2009, comprobando que constan trece solicitudes, todas ellas tiene dirección de correo de origen en el dominio “cfnavarra.es”. Se ha comprobado que una de las solicitudes corresponde al colegio público Patxi Larraizar, de fecha 29 de enero de 2009, solicitando el censo de los nacidos en el año 2006 y la contestación de fecha 3 de febrero de 2009 remitiéndole la información solicitada.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

La denuncia se concreta en el tratamiento de los datos de un menor sin el consentimiento de sus padres. El artículo 6 de la LOPD dispone: *"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa*.
Añadiendo el apartado 2 del citado artículo que *"no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*
El tratamiento de datos de carácter personal tiene que contar con el consentimiento del afectado o, en su defecto, debe acreditarse que los datos provienen de fuentes accesibles al público, que existe una Ley que ampara ese tratamiento o una relación contractual o negocial entre el titular de los datos y el responsable del tratamiento que sea necesaria para el mantenimiento del contrato.
El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F.J. 7 primer párrafo) *"consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)".*
Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

III

La Agencia Española de Protección de Datos contestó, a través del Gabinete Jurídico, una consulta acerca del mismo asunto que los hechos denunciados, sobre si resultaría conforme a lo dispuesto en la LOPD, la obtención de datos del Padrón Municipal de Habitantes por un centro público de enseñanza para realizar un envío de información referida al mismo a los hogares en que residan niños en edad de escolarización. El informe indicaba lo siguiente:

La comunicación de datos solicitada constituye, conforme a lo dispuesto en el artículo 3 i) de la citada Ley Orgánica, una cesión de datos de carácter personal, definida como "Toda revelación de datos efectuada a persona distinta del interesado". Tal y como determina el artículo 11.1 de la Ley Orgánica 15/1999, "los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado". Esta regla de consentimiento sólo se verá exceptuada en los supuestos contemplados en el artículo 11.2, entre los que cabe destacar aquellos casos en que una norma con rango de Ley dé cobertura a la cesión. Por ello, deberá determinarse si la legislación reguladora de los ficheros a los que la consulta se refiere permite esa transmisión de sus datos.

Por otro lado, siendo el Padrón un fichero de titularidad pública, debe partirse, el principio de delimitación de la finalidad en las cesiones entre Administraciones Publicas consagrado por el artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, al exigir que si los datos son cedidos a otras Administraciones Publicas sirvan sólo para el ejercicio de competencias iguales o que versen sobre materias semejantes, con la única excepción, tras la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, de que el cambio de finalidad esté fundado en una de las causas contenidas en el artículo 11 de la propia Ley Orgánica, pudiendo ser sustituida la necesidad del consentimiento para el cambio de finalidad por una previsión realizada en una disposición con rango de Ley (art.11.2 a).

En cuanto al Padrón municipal, el artículo 16.3 de la Ley reguladora de las bases del régimen local, redactado conforme a lo establecido en la Ley Orgánica 14/2003, de 20 de noviembre, dispone que "los datos del Padrón municipal se cederán a otras Administraciones Públicas que lo soliciten sin consentimiento previo del afectado solamente cuando les sean necesarios para el ejercicio de sus respectivas competencias, y exclusivamente para asuntos en los que la residencia o el domicilio sean datos relevantes. También pueden servir para elaborar estadísticas oficiales sometidas al secreto estadístico, en los términos previstos en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública".

Fuera de estos supuestos, los datos del Padrón son confidenciales y el acceso a los mismos se rige por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

A la vista de lo dispuesto en el precepto transcrito y el artículo 27.5 de la Constitución Española que dispone "Los poderes públicos garantizarán el derecho de todos a la educación mediante un programación general de la enseñanza con participación efectiva de todos los afectados y la creación de centros docentes", podemos concluir que la comunicación de los datos a los que se refiere la consulta dado que se efectuará a un colegio público, que depende de la consejería de educación del Ayuntamiento consultante y siendo el domicilio un requisito fundamental a la hora de escolarizar a los niños, dicha comunicación podrá considerarse amparada en lo dispuesto en el artículo 11.2 a) de la Ley Orgánica 15/1999".

Por tanto, la cesión realizada por el Instituto de Estadística de Navarra a la escuela Pública Patxi Larrainzar se encuentra amparada por la normativa reseñada y, en consecuencia, el envío que realizó la Escuela a la familia con un niño que iniciaría su escolarización también cumple la normativa de protección de datos ya que el consentimiento para dicho tratamiento está habilitado en una Ley, no siendo necesario el consentimiento del afectado.

Durante las actuaciones previas de investigación efectuadas, se han recogido múltiples manifestaciones, algunas de ellas contradictorias, pero las únicas acreditaciones documentales que se han constatado son que el Instituto de Estadística

de Navarra envió el censo de los nacidos en el año 2006 a la Escuela Pública Patxi Larrainzar y que el denunciante recibió en su domicilio un sobre con el membrete del Gobierno de Navarra y del Colegio Público de Educación Infantil y Primaria Patxi Larrainzar, con un tríptico de la educación en el mencionado Centro Público. Como se ha señalado, la cesión y el tratamiento realizado cumplen las obligaciones establecidas en la LOPD.
Por lo tanto, de acuerdo con lo señalado, **Por el Director de la Agencia Española de Protección de Datos,**

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a la APYMA COLEGIO PUBLICO PATXI LARRAINZAR, a la ESCUELA PUBLICA PATXI LARRAINZAR, a la FEDERACIÓN SORTZEN-IKASBATUAZ, al INSTITUTO DE ESTADÍSTICA DE NAVARRA y a DON ***A.A.A.***.
De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.
Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de 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 citada 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.

Expediente Nº: E/02022/2009

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante DON A.A.A., en virtud de las denuncia presentadas ante la misma por tres denunciantes, y en base a los siguientes

HECHOS

PRIMERO: Con fechas 27 y 28 de abril de 2009, tuvieron entrada en esta Agencia tres escritos remitidos por tres denunciantes, en los que se declaran lo siguiente:
- Durante los años 2006-2007 (denunciante 1), 2007 y 2008 (denunciante 2) y 2006-2007 y 2008 (denunciante 3), cursaron estudios en el I.E.S. "Vicente Blasco Ibáñez" de Valencia. Asimismo, durante el año 2005 asistieron al curso de perfeccionamiento de la academia Centro de Formación Electrónica e Industrial, S.L., CFEI, sito en Benimamet (Valencia).
- Sin intervención de los denunciantes, el día 27 de mayo de 2008, el profesor Don A.A.A., presentó en el Registro del Instituto una denuncia contra otro profesor, en la que identificaba a los denunciantes, junto a otros estudiantes más, indicando nombre, apellidos y D.N.I., como estudiantes que se habían beneficiado de asistir a los dos centros antes indicados y haber obtenido calificación privilegiada en el I.E.S. En la denuncia se dice textualmente *"Adjunto algunos nombres de alumnos que se matricularon en la academia, y de ellos algunos se presentaron a examen en el ÍES, (se podrán comprobar por las actas del instituto las calificaciones y el tiempo que tardaron en sacarse el título de Técnico Auxiliar en electricidad)".*
- Los datos de los estudiantes únicamente pueden haber sido facilitados por el responsable de los archivos y registros de la academia CFEI, quien, al parecer, mantiene un conflicto personal con el profesor acusado de facilitar el aprobado de los exámenes a los alumnos señalados.
- Tras conocer los denunciantes el contenido de aquel escrito, con fecha 12 de septiembre de 2008, remitieron a los denunciados, una carta reclamando la información sobre los datos que cada uno de ellos poseen, su legitimación para usarlos, la forma en que fueron obtenidos, el contenido exacto de los archivos y el tratamiento que se les está dando. Todo ello al objeto de poder ejercer los derechos de oposición, rectificación y cancelación, en su caso.
Acompañan a la denuncia copia de la carta remitida al "Instituto E.S. Vicente Blasco Ibáñez", copia de la carta remitida al CFEI, CENTRO DE FORMACIÓN ELECTRÓNICA INDUSTRIAL, S.L., y copia de la carta remitida al profesor Don A.A.A., con el sobre devuelto ya que eludió su recepción, a buen seguro advertido de su contenido por su cooperador, según manifiestan los denunciantes.
- El Instituto de Enseñanza Secundaria Vicente Blasco Ibáñez contestó cumplidamente y declaró que se realizarían las actuaciones necesarias con el fin de averiguar si se había producido un uso indebido de la información por parte de algún miembro de la comunidad educativa.
- La entidad CFEI, firmada por su representante legal, Don B.B.B., contestó a la carta requerimiento alegando que la sociedad estaba disuelta y que los datos habían sido destruidos.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

a. Entre la documentación aportada por los denunciantes se encuentra copia del escrito presentado por D. A.A.A. ante el IES Vicente Blasco Ibáñez con el que adjunta copia del escrito presentado ante la Consejería de Educación de la Generalitat Valenciana.
En dicho escrito se incluyen nombre, apellidos, DNI y año académico de dieciocho personas entre las que se encuentran los tres denunciantes, expresándose que en el citado I.E.S. se cometen actos que pudieran ser constitutivos de un delito, dado que el Jefe del Departamento de Electricidad, Sr. C.C.C., es, además, accionista del Centro de Formación Electrónica e Industrial (CFEI), centro en el que se han formado las personas incluidas en el escrito y luego éstos se examinaban en el I.E.S. para obtener el carnet de instalador, siendo examinados por el propio Sr. C.C.C..
b. Tras solicitar por parte de la Inspección de Datos de la Agencia información a Don A.A.A. en relación con los hechos denunciados, éste contestó lo siguiente: - El origen de los datos se refleja en las páginas 1 y 2 del escrito presentado a la Consellería de Educación. Estos datos fueron expresados en mayo de 2005 por el Sr. D. C.C.C., que actuaba como profesor y accionista en el CENTRO DE FORMACIÓN ELECTRÓNICA E INDUSTRIAL (CFEI) y también en esa época era profesor y jefe de departamento de electricidad en el ÍES "Vicente Blasco Ibáñez".
- Ha tenido conocimiento de que D. D.D.D., D. E.E.E. y D. F.F.F., han sido alumnos el CENTRO DE FORMACIÓN ELECTRÓNICA E INDUSTRIAL (CFEI), por el interés que mostró el Sr. C.C.C. en los Sres. referenciados.
- No ha existido ningún tratamiento de datos, ya que los datos de las personas que se examinan son públicos y se exponen en los tablones del Instituto en los meses de Junio-Julio y Septiembre (a fecha del escrito, aún continúan publicados los datos de los alumnos de Septiembre de 2009). Nunca ha tenido vinculación con los Sres. mencionados en las hojas aludidas, ni tampoco ha tenido relación de ningún tipo con CENTRO DE FORMACIÓN ELECTRÓNICA E INDUSTRIAL (CFEI).
- Cuando tuvo conocimiento de que el Señor C.C.C. había tenido una participación en una academia y era administrador de otra, al suponer que esto podría perjudicar a los alumnos mencionados, al Instituto y al Departamento, lo puso en conocimiento de la Inspectora de Educación. Los datos que se presentan en el escrito que va dirigido exclusivamente a la Inspectora de Educación son públicos, datos a los que ella tiene acceso. Además el escrito se hace por vía de régimen interno, sin dar publicidad de lo acontecido.
- Por otra parte, como funcionario, tiene la obligación de velar que se cumpla lo dispuesto en Artículo 48.2. del Régimen Jurídico de la Función Pública Valenciana.
- El documento objeto de la denuncia estaba exclusivamente destinado a la Sra. Inspectora de Educación, por lo que desconoce cómo los tres denunciantes han tenido acceso al mismo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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

Los denunciantes concretan su denuncia en la comunicación de sus datos personales por parte del Centro de Formación Electrónica e Industrial, del cual fueron alumnos, a

Don A.A.A.. Este último los ha trasladado a la Consejería de Educación de la Generalitat Valenciana.
De acuerdo con lo manifestado por el Sr. A.A.A., los datos de los denunciantes, sí como de otras personas, se los facilitó un profesor del IES Vicente Blasco Ibáñez y también profesor del CFEI, Sr. C.C.C., en el mes de mayo de 2005.
En consecuencia, procede examinar lo que la LOPD regula para la cesión de datos. Así, el artículo 11.1 dispone: "*1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."*
El artículo 44.4.b) de la LOPD, considera infracción muy grave: *"La comunicación o cesión de los datos de carácter personal, fuera de los casos en los que estén permitidas".*
El artículo 47 de la LOPD, bajo el epígrafe *" Prescripción",* establece: *"1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año. 2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido. 3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor."*
Según consta en la propia denuncia presentada y en la documentación que se ha obtenido durante las Actuaciones Previas de Investigación, los hechos valorados en las presentes actuaciones, relacionados con la cesión de los datos de los alumnos denunciantes por parte de CFEI al Sr. A.A.A., se remontan al mes de mayo de 2005, habiendo tenido esta Agencia conocimiento de los mismos por virtud de la citada denuncia registrada de entrada en el Organismo en fecha 27 de abril de 2009.
Así, considerando que el plazo de prescripción comienza a contarse el día en que se cometió la presunta infracción, en el presente caso el *"dies a quo"* del cómputo prescriptivo debe fijarse en el mes de mayo de 2005, resultando que la posible infracción del deber de secreto o cesión denunciada, o cualquier otra que pudiera derivarse de estos hechos, con independencia de su calificación, ha prescrito de conformidad con lo dispuesto en el mencionado artículo 47.1 de la LOPD, que establece unos plazos de prescripción de tres años para las infracciones muy graves, dos para las graves y un año para las leves, ya finalizados cuando la denuncia respectiva tuvo entrada en esta Agencia Española de Protección de Datos.
Teniendo en cuenta, además, que de conformidad con lo dispuesto en el apartado 3 del precepto antes citado, así como en el artículo 132.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPCA), el único modo de interrumpir el computo del plazo de prescripción es la iniciación, con conocimiento del interesado, del oportuno procedimiento sancionador, y en el presente caso, al no haber tenido conocimiento de los hechos con anterioridad, no ha sido posible formalizar dicha incoación dentro de plazo establecido, procede declarar la prescripción de la presunta infracción.
En cuanto a la inclusión de sus datos personales en la denuncia presentada por Don A.A.A. ante la Consejería de Educación, los datos de los alumnos del I.E.S. son conocidos por la Consejería de Educación de la Comunidad Autónoma donde está ubicado, por lo que no se produce ninguna vulneración del deber de guardar secreto al tratarse de datos ya conocidos. Además, se han transmitido en el marco de una denuncia y a una Administración que tiene obligación de guardar secreto. Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución a DON A.A.A., y a los tres denunciantes. 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 e 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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de 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 citada 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.

Procedimiento Nº PS/00115/2007

RESOLUCIÓN: R/00996/2007

En el procedimiento sancionador PS/00115/2007, instruido por la Agencia Española de Protección de Datos a la entidad **C.C.C. Y OTRA C.B.**, vista la denuncia presentada por **DÑA. G.G.G.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 23/05/2005, tuvo entrada en esta Agencia un escrito de Dña. G.G.G. (en lo sucesivo la denunciante), en los que denuncia que en el diario *"La Voz de Galicia"* del día dd/mm/aaaa se publicó un anuncio del Centro de Estudios *"La Academia"*, cuya razón social es C.C.C. y otra C.B. (en lo sucesivo LA ACADEMIA), en el que se incluyen su nombre y dos apellidos. La denunciante manifiesta que no ha prestado su consentimiento para que sus datos personales fueran insertados en el citado anuncio, como si se tratase de una alumna de LA ACADEMIA, con la que no ha mantenido relación alguna, salvo el envío de una solicitud de información sobre las matrículas del centro.
Aporta copia del anuncio publicado en el diario citado, en el que aparecen los fatos de la denunciante entre *"los opositores que superaron las pruebas en la última convocatoria de la Xunta"* para la obtención de una plaza de arquitecto técnico.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos, que constan en el escrito remitido por LA ACADEMIA en fecha 28/09/2005:
1. La denunciante no ha sido alumna de LA ACADEMIA, por lo que sus datos no se han incluido en ningún fichero de dicha entidad.
2. El nombre y apellidos de la denunciante se incluyó en el anuncio publicado por LA ACADEMIA en el diario *"La Voz de Galicia"* por error, ya que figuraba junto al de otros opositores en los listados de resultados de las pruebas selectivas para cubrir varias plazas de Arquitectos Superiores y Técnicos en la Xunta de Galicia, publicados en el Diario Oficial de Galicia y en Internet.

TERCERO: Con fecha 23/04/2007, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a LA ACADEMIA por la presunta infracción del artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como grave en el artículo 44.3.d) de dicha norma.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento sancionador, LA ACADEMIA presenta escrito en el que, después de advertir sobre la falta de concreción del acuerdo de inicio, en relación con la infracción que se imputa, que considera causante de indefensión y la nulidad de dicho acuerdo, señala que la inclusión, por error, del nombre y apellidos de la denunciante en un anuncio publicado en el diario *"La Voz de Galicia"* no constituye un tratamiento de datos comprendido en la normativa que regula dicha materia, por cuanto se trata de información que figura en fuentes de acceso público, tales como los tablones de anuncios de la Xunta de Galicia y su web oficial, así como en el Diario Oficial. Dichos datos, además, no se recogieron en fichero alguno, automatizado o no, ni se conservan por la entidad. A este respecto, el artículo 3.1 de la directiva 95/46/CE, de la que trae causa la LOPD, establece que

"las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".
En el presente caso, únicamente ha existido un tratamiento manual, que resulta del listado enviado a la agencia de publicidad Reclam, Publicidad & Marketing y Artes Gráficas, S.A. (en lo sucesivo RECLAM), que elaboró el anuncio, que recoge el nombre y apellidos de todos los opositores que superaron las pruebas de una convocatoria realizada por la Xunta de Galicia y que coincide con el listado publicado por esta misma entidad.
En el listado remitido por LA ACADEMIA a RECLAM se señalaron, mediante una marca, los opositores que habían sido alumnos de la misma. Sin embargo, el empleado de dicha agencia encargado de elaborar el anuncio transcribió, por error, los datos de todos los opositores y no únicamente los de los alumnos de LA ACADEMIA.
Finalmente, advierte que la infracción que se imputa ha prescrito por el transcurso de dos años, a contar desde la fecha en que tuvo lugar el tratamiento de datos que se imputa, que coincide con el envió del listado a la agencia de publicidad el 15/04/2005, y hasta la notificación de apertura del procedimiento, en fecha 25/04/2007.

QUINTO: En fecha 08/06/2007, se acordó por el Instructor del procedimiento la apertura de un período de pruebas, teniéndose por reproducida la documental aportada por la denunciante, así como las actuaciones previas de investigación desarrolladas por la Inspección de Datos de esta Agencia Española de Protección de Datos, E/00602/2005. Asimismo, en atención a lo solicitado por LA ACADEMIA, se acordó requerir a RECLAM para que aportase a esta Agencia Española de Protección de Datos testimonio en el que se de respuesta a las siguientes cuestiones: *"Que manifieste que fue el personal de dicha Empresa (RECLAM) la que efectivamente confección el anuncio, en esta y en las demás ocasiones que se publica un anuncio de estas características.*
*Que, como es habitual, en el listado en papel –extraído directamente de una fuente de accesible al público.- que LA ACADEMIA envió a RECLAM aparecían destacados, de entre el resto, los opositores que se habían preparado en La Academia señalados con un signo del tipo "**.**". Que al pasar a mano la Agencia RECLAM el listado público, se incluyó por un simple error mecanográfico el nombre de la denunciante. Que el listado público se le remitió por fax con una semana de antelación a la publicación del anuncio"*.
En respuesta a estas cuestiones, el Director Financiero de RECLAM manifestó lo siguiente: *"1.- Efectivamente fue el personal de esta empresa el que confeccionó el anuncio en esta y en otras ocasiones.*
2.- Igualmente, en el listado que remite el anunciante "La Academia" se identifican con el indicado signo los que deben incluirse en el anuncio.
3.- Al trasladar los datos de la lista en la confección del anuncio se incluyó el nombre de la denunciante porque apareció una marca que se identificó como similar al signo referido al margen de dicho nombre que se entendió como una señal para su inclusión y que según parece fue error del mecanismo de transmisión en el medio de comunicación habitual (vía fax) con "La Academia".
4.- Es cierto que el listado se remitió con una semana de antelación a la publicación, como es habitual en relación a este anunciante y por vía fax, como se acaba de referir".

SEXTO: Transcurrido el período de pruebas, se inició el trámite de audiencia, concediéndose a LA ACADEMIA la posibilidad de obtener copia de los documentos que integran las actuaciones y plazo para formular las alegaciones que considerase oportunas, que transcurre sin que se presentara escrito alguno.

SÉPTIMO: Con fecha 20/09/2007, se emitió propuesta de resolución en el sentido de que por el Director de la Agencia Española de Protección de Datos se sancionase a LA ACADEMIA con multa de 60.101,21 (sesenta mil ciento un euros con veintiún céntimos) por la infracción de del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma. Notificada la citada propuesta, se recibe escrito de alegaciones en el que la entidad LA ACADEMIA se reitera, básicamente, en sus alegaciones anteriores.

HECHOS PROBADOS

PRIMERO: La entidad C.C.C. y otra C.B. dispone de un centro de enseñanza, denominado *"La Academia"*, en el que se imparten clases preparatorias de pruebas selectivas convocadas por la Administraciones Públicas.

SEGUNDO: Dña. G.G.G. no ha sido alumna del centro de enseñanza *"La Academia"* que dirige la entidad C.C.C. y otra C.B..

TERCERO: No consta que los datos personales de Dña. G.G.G. figuren registrados en los ficheros de alumnos pertenecientes al centro "La Academia".

CUARTO: Los datos personales de Dña. G.G.G., relativos a nombre, apellidos y DNI, aparecieron publicados en el Diario Oficial de Galicia de fecha dd/mm/aaaa, incluido en el listado de personas que superaron las pruebas convocadas por la Xunta de Galicia para acceso al Cuerpo Facultativo de Grado Medio, Escala de Arquitectos Técnicos, publicado como Anexo a la Resolución de fecha 13/01/2003, del Tribunal designado para calificar dicho proceso selectivo, con el detalle de la puntuación obtenida en la fase de concurso.

QUINTO: En el diario *"La Voz de Galicia"* del día dd/mm/aaaa se publicó un anuncio del Centro de Estudios *"La Academia"*, cuya razón social es C.C.C. y otra C.B., en el que se incluyeron los datos personales de Dña. G.G.G., relativos a nombre y dos apellidos, entre *"los opositores que superaron las pruebas en la última convocatoria de la Xunta"* para la obtención de una plaza de arquitecto técnico.

SEXTO: Dña. G.G.G. no prestó su consentimiento para que sus datos personales fueran insertados en el anuncio publicado por C.C.C. y otra C.B. en el diario *"La Voz de Galicia"* del día dd/mm/aaaa, como si se tratase de una alumna del centro "La Academia", con la que no ha mantenido relación alguna, salvo el envío de una solicitud de información sobre las matrículas del centro.

SÉPTIMO: C.C.C. y otra C.B. remitió a la agencia de publicidad Reclam, Publicidad & Marketing y Artes Gráficas, S.A., contratada por aquella entidad para que se encargar de la publicación del anuncio reseñado en el Hecho Probado Quinto, un listado con el nombre y apellidos de los opositores que habían superado las pruebas de la convocatoria efectuada por la Xunta de Galicia, incluidos los relativos a Dña. G.G.G.. Reclam, Publicidad & Marketing y Artes Gráficas, S.A. ha declarado que el envío de aquel listado se realizó con una semana de antelación a la publicación del anuncio en fecha dd/mm/aaaa. Asimismo, Reclam, Publicidad & Marketing y Artes Gráficas, S.A. ha declarado que la inserción en el mismo de los datos personales de Dña. G.G.G. se debió a un error cometido por el personal de la propia agencia en la confección de dicho anuncio.

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

Con carácter previo al examen de la cuestión de fondo, procede analizar la excepción alegada por LA ACADEMIA sobre la prescripción de la infracción que se imputa. Considera la citada entidad que la infracción ha prescrito, por el transcurso de más de dos años, contados desde el día 15/04/2005, fecha del envío a la agencia de publicidad RECLAM del listado de personas que debían insertarse en el anuncio publicado en el diario *"La Voz de Galicia"*, , y hasta la notificación de la apertura del presente procedimiento sancionador, que tuvo lugar en fecha 25/04/2007.
La LOPD, en el artículo 47.1, 2 y 3, establece: *"1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.*
2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.
3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor". Por otra parte, como señala el artículo 132.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC), *"El plazo de prescripción de las infracciones comenzará a contarse desde el día que la infracción se hubiera cometido. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador"*.
El presente supuesto tiene por objeto el examen de unos hechos supuestamente constitutivos de infracción al artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma. Por tanto, de acuerdo con las normas indicadas, las infracción que se analiza prescribe en el plazo de dos años contados desde el día en que la infracción se hubiera cometido.
En relación con esta presunta infracción, no pueden tenerse en cuenta las alegaciones formuladas sobre la prescripción de la misma. La infracción que se imputa resulta de la utilización de los datos personales de la denunciante en un anuncio publicitario de LA ACADEMIA, insertado en el diario *"La Voz de Galicia"* del día dd/mm/aaaa. Por tanto, en el momento en que tiene lugar la notificación de apertura del procedimiento, en fecha 25/04/2007, no habían transcurrido los dos años establecidos para que opere el instituto de la prescripción, de modo que la infracción que se imputa no había prescrito el día en que fue notificado el inicio del presente procedimiento sancionador.

III

Se imputa a LA ACADEMIA en el presente procedimiento la comisión de una infracción del artículo 6.1 de la LOPD, que dispone que *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*. El apartado 2 del mencionado artículo contiene una serie de excepciones tasadas a la regla general contenida en el 6.1: *"No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato, de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o*

cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

A este respecto, debe señalarse que el artículo 3.c) de la LOPD define el tratamiento de datos como *"Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"*.

El tratamiento de datos sin consentimiento de los afectados o sin otra habilitación amparada por la Ley constituye una vulneración del derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre (F.J. 7, primer párrafo), *"consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

En el presente caso, ha quedado acreditado que la denunciante no ha mantenido ninguna relación con el centro de estudios LA ACADEMIA ni consintió que la misma tratara sus datos personales con finalidad alguna. A pesar de ello, LA ACADEMIA sometió a tratamiento los datos de carácter personal de la denunciante, relativos a nombre y apellidos, para insertarlos en un anuncio publicado por dicho centro de estudios en el diario *"La Voz de Galicia"* del día dd/mm/aaaa, en el que se relacionan los alumnos del mismo que superaron unas pruebas selectivas convocadas por la Xunta de Galicia para la obtención de una plaza de arquitecto técnico.

LA ACADEMIA no ha aportado prueba documental alguna que acredite el consentimiento de la denunciante para que dicha entidad pudiera llevar a cabo el mencionado tratamiento de datos, antes bien, los documentos que obran en el procedimiento y las manifestaciones realizadas por la propia entidad imputada, evidencian que la misma no contaba con el consentimiento del denunciante.

Cabe decir por tanto que, ante la falta de acreditación del consentimiento de la denunciante para el tratamiento de datos personales realizado, y ante la ausencia de cobertura legal que amparase dicho tratamiento sin consentimiento, se considera infringido el artículo 6.1 de la LOPD, siendo imputable dicha infracción a la entidad LA ACADEMIA como responsable del tratamiento de datos personales efectuado, en la medida en que dicha entidad decidió la finalidad, contenido y uso del tratamiento.

IV

La hoy derogada Ley Orgánica 5/1992, de 29/10, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en lo sucesivo LORTAD), delimitaba su ámbito de aplicación en torno al concepto de fichero automatizado (artículo 2), que figuraba definido como *"todo conjunto organizado de datos de carácter personal que*

sean objeto de tratamiento automatizado (...)". Congruentemente con dicha configuración legal, la LORTAD se limitaba a definir la figura del responsable del fichero (artículo 3.b) y d)).

Por el contrario, la vigente LOPD ha modificado el ámbito de aplicación objetivo de la norma circunscribiéndola a *"los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento automatizado, y a toda modalidad de uso posterior a estos datos (...)"* (artículo 2). De acuerdo con esta delimitación, la LOPD modifica la definición del fichero y diferencia las figuras del responsable del fichero y del responsable del tratamiento (artículo 3.b. y d.). Asimismo delimita con precisión la figura del encargado del tratamiento (artículo 12). Efectivamente, el artículo 3 de la LOPD establece lo siguiente: *"b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

"d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

Esta modificación es congruente con las exigencias de la Directiva 95/46/CE, de 24 de octubre, 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, que la LOPD incorpora a nuestro derecho, conforme a la cual, en el caso de los datos personales susceptibles de tratamiento automatizado, la Ley se aplica no sólo cuando existe un conjunto organizado (fichero) de dichos datos, sino también cuando se realizan operaciones y procedimientos que permitan la recogida, grabación, conservación, elaboración, bloqueo y cancelación de aquellos, aunque el responsable de ese tratamiento carezca de bases de datos de su titularidad que, de acuerdo con los términos legales, se incluyen en la definición de fichero.

Conforme se ha señalado, cabe que el sistema de protección de la LOPD se exija a los responsables del tratamiento, aunque carezcan de ficheros, e incluso, a los meros encargados de aquél, a los que la LOPD también puede convertir en responsables (art. 12.4). Una interpretación contraria llevaría a que el sistema de protección de datos pudiera quedar vacío de tutela respecto de un número cada vez mayor de tratamientos que se externalizan.

El Tribunal Supremo, en su Sentencia de 26/01/2005, dictada en casación para unificación de doctrina, confirma la doctrina anteriormente expuesta al señalar que *<<junto al responsable del fichero –que era en la Ley 5/1992- quien estaba sujeto al régimen sancionador establecido en dicha ley (art. 42) en la nueva Ley 15/1999 aparece un nuevo personaje, el responsable del tratamiento, como posible sujeto pasivo de la potestad sancionadora de la que hoy se llama –a partir de la Ley 62/2003, de 30 de diciembre- Agencia Española de Protección de Datos (artículo 43), Véase lo que dicen uno y otro precepto: Ley 5/1992 "Art. 42. Responsables: 1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley". Ley 15/1999 " Art. 43. Responsables: 1- Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente ley". Y esto es así porque la nueva Ley Orgánica –a diferencia de la vieja Ley Orgánica, que atribuía la potestad de decidir sobre la finalidad, contenido y uso del tratamiento únicamente al responsable del fichero- reconoce que esa decisión pueda tomarla –y así ocurre muchas veces el responsable del tratamiento.*

He aquí el nuevo texto: Ley 15/1999 "As rtículo 3. A los efectos de la presente Ley se entenderá por: [...] d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

No se trata como se ve de un mero cambio de redacción, de un simple giro gramatical, o una innovación puramente estilística. Es algo más profundo: estamos ante un cambio esencial en el modo de afrontar la regulación de las relaciones que se entablan entre quienes manejan los datos y el titular de los mismos>>.

En este mismo sentido se pronuncia la Audiencia Nacional en su Sentencia de 03/03/2004, citada entre otras en su Sentencia de 18/01/2006, al señalar que <<*el tipo sancionador previsto en el artículo 44.3.d) de la Ley Orgánica 15/1999, castiga "tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley", como el previsto en el artículo 4.3 de la citada Ley que impone la veracidad y exactitud de los datos de carácter personal. Acorde con este principio se establecen una serie de obligaciones, tendentes a alcanzar esa veracidad y exactitud de los datos de carácter personal que se encuentran en el fichero, y cuyo incumplimiento es digno de reproche y configura una infracción administrativa por la que se impone la sanción que se recurre. Dicho de otra forma, el medio de conseguir que los principios en que se inspira esta regulación sobre la protección de datos –al amparo del artículo 18.4, más allá del contenido del artículo 18.1 de la CE, como un derecho fundamental autónomo tras la STC 292/2000 –sean efectivos es mediante la acción sancionadora, es decir, tipificando las conductas que impidan el cumplimiento de los expresados principios. El ámbito subjetivo del ilícito administrativo descrito son los "responsables de los ficheros y los encargados de los tratamientos", pues sólo a éstos les es aplicable el régimen sancionador que diseña la Ley Orgánica 15/1999, ex artículo 43.1 de la misma Ley. Esta delimitación subjetiva, ha sido ampliada en la Ley Orgánica 15/1999, a la sazón aplicable, respecto de la prevista en la Ley Orgánica 5/1992, en cuyo artículo 42.1 sólo sometía a su régimen sancionador a los responsables de los ficheros. Ahora bien, debe tenerse en cuenta que el responsable del fichero tiene una configuración más amplia en la Ley de 1999 que en la de 1992, pues sólo así puede explicarse que cuando el artículo 43.1 alude al "responsable del fichero", esta expresión comprende ahora al responsable del tratamiento, ex artículo 3.d) de la Ley Orgánica 15/1999, bajo la expresión "responsable del fichero o tratamiento", desconocida en la Ley de 1992, y si bien es cierto que las definiciones son coincidentes antes y ahora, sin embargo se ha incluido en la vigente Ley a aquellos otros que decidiendo sobre la finalidad, contenido y uso del tratamiento, no sean propiamente responsables del fichero. Entendemos, por tanto, por responsable del fichero o del tratamiento la persona física o jurídica, que decida sobre la finalidad, contenido y uso del tratamiento; y por encargado del tratamiento quien trate datos personales por cuenta del responsable del tratamiento, según define el artículo 3, apartados d) y g), respectivamente, de la Ley Orgánica 15/1999>>*.

Dentro de la doctrina expuesta, en el presente caso, ha quedado acreditado que el tratamiento de los datos de la denunciante se realizó por encargo de LA ACADEMIA. Por ello, resulta acreditado que quien decidió, en definitiva, sobre la finalidad, contenido y uso del mismo fue LA ACADEMIA. Por tanto, ha cometido una infracción de lo dispuesto en el artículo 6.1 de la LOPD, por cuanto dicha entidad es responsable del tratamiento de los datos personales de la denunciante, que se efectuó sin contar con su consentimiento, y sin que concurriera ninguna de las causas de exclusión del consentimiento contempladas en el artículo 6.2 de la LOPD.

La Sentencia de la Audiencia Nacional de 28/01/2004 establece en su Fundamento de Derecho Cuarto que *"... se incurre en la conducta antes descrita, a pesar de la externalización de servicios, siempre que se haya intervenido decidiendo sobre el tratamiento de los datos y su aplicación, y, además, que el responsable, en este caso, del tratamiento haya podido extremar su diligencia para tener constancia de que los datos empleados habían sido recabados con el consentimiento de los titulares de los mismos, lo que se relaciona con la culpabilidad de la conducta por la que se sanciona"*.

Finalmente, cabe señalar que la obtención de los datos de la denunciante de fuente de acceso público no modifica la conclusión anterior, por cuanto la utilización posterior de los mismos con fines publicitarios para LA ACADEMIA supone un tratamiento sin consentimiento.

V

El artículo 44.3.d) de la LOPD tipifica como infracción grave: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*.
La Audiencia Nacional ha manifestado en su Sentencia de 22/10/2003 que *"... la descripción de conductas que establece el artículo 44.3.d) de la Ley Orgánica 15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cual es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave "tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley", por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizadamente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos, realizando envíos publicitarios"*.
En este caso, LA ACADEMIA ha incurrido en la infracción descrita ya que el consentimiento para el tratamiento de los datos personales es un principio básico del derecho fundamental a la protección de datos, recogido en el artículo 6 de la LOPD. La entidad mencionada ha tratado los datos de la afectada sin contar con su consentimiento, lo que supone una vulneración de este principio, conducta que encuentra su tipificación en este artículo 44.3.d) de la citada Ley Orgánica.

VI

El artículo 45.2, 4 y 5 de la LOPD establece: *"2. Las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 euros"*. *"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.*
5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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 relación con la aplicación del artículo 45.5 de la LOPD, la Audiencia Nacional ha señalado, entre otras, en Sentencia de 27/10/2004, que *"..el citado precepto concreta el principio de proporcionalidad (reconocido para el Derecho administrativo sancionador, con carácter general, en el art. 131.3 de la Ley 30/1992), permitiéndose la disminución en un grado de la sanción aplicable en casos de cualificada disminución de la culpa o de la antijuridicidad. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor de justicia (art. 1.1 CE), por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos..."*. Así, el artículo 45.5 de la LOPD debe aplicarse de forma excepcional y cuando se den suficientes circunstancias para ello. En el presente procedimiento, atendidas las manifestaciones realizadas por la agencia de publicidad encargada de la realización del anuncio determinante del tratamiento de datos sin consentimiento, se aprecian circunstancias que suponen una disminución cualificada de la culpabilidad. Estas circunstancias, sin embargo, no exoneran de responsabilidad a LA ACADEMIA, por la falta de diligencia que resulta de no elaborar un listado específico de las personas que debían insertarse en el anuncio contratado que recogiera, únicamente, los datos de aquellas que hubiesen prestado su consentimiento para ello. Por otra parte, en relación con los criterios de graduación recogidos en el citado artículo 45.4 y, en especial, a la falta de intencionalidad acreditada en el procedimiento, procede la imposición a LA ACADEMIA de una sanción de 6.000 euros. Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: IMPONER a la entidad **C.C.C. Y OTRA C.B.**, por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 6.000 (seis mil euros), de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: NOTIFICAR la presente resolución a **C.C.C. Y OTRA C.B.**, con domicilio en (c/.....), y a **DÑA. G.G.G.**, con domicilio en (c/.....).

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior. 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.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Procedimiento Nº PS/00259/2008

RESOLUCIÓN: R/00614/2008

En el procedimiento sancionador PS/00259/2008, instruido por la Agencia Española de Protección de Datos a **D. S.S.S.**, vista la denuncia presentada por la **POLICIA LOCAL DE OURENSE** y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 9 de mayo de 2007, tuvo entrada en esta Agencia un escrito de de la Policía Local de Ourense en el que declara que ha sido localizado en una red de intercambio de ficheros P2P disponible en Internet (entorno compartido *E-mule*), un fichero denominado *"(...X.....)",* que contiene datos de 1.250 alumnos de un centro que posiblemente gestiona PROINSSA en (.....). El fichero es compartido, de acuerdo a los datos aportados, por un usuario denominado *"(***V***)"* con dirección IP ##########.
A la denuncia se aporta diversa documentación, entre la que se encuentra copia completa del fichero encontrado. Los datos de los alumnos se refieren a su nombre y apellidos, dirección, teléfono, fecha de nacimiento y DNI.

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

1. Mediante consulta realizada a la entidad Telefónica de España, S.A.U., que la dirección IP responsable de compartir el fichero en la fecha señalada tenía como titular en el momento de la localización del fichero a D. S.S.S., domiciliado en (C/.....).

2. La entidad PROMOCIÓN DE INICAITIVAS SOCIO-SANITARIAS, S.L.L. (en lo sucesivo PROINSSA) realizó servicios de consultoría para la ASOCIACIÓN FORTE, consistentes en la puesta en marcha y gestión del Centro de Acceso Público a Internet (en lo sucesivo CAPI) ubicado en la localidad de (.....), provincia de (……). La prestación del servicio se realizó en el periodo comprendido entre septiembre de 2002 y Julio de 2005.
Para facilitar la gestión del Centro, PROINSSA creó un fichero, denominado *"CAPI-USUARIOS",* con la finalidad de gestionar los datos de inscripción de los usuarios del CAPI. Dicho fichero fue inscrito en el Registro General de Protección de Datos en fecha 5 de marzo de 2003 y con el código ########.
El CAPI contaba con un sistema de información consistente en una red de área local con acceso a Internet en la que convivían dos servidores y una serie de ordenadores personales instalados en las aulas. Además, se contaba con un ordenador personal en la zona de recepción en el que residía la copia de trabajo del fichero *"CAPI-USUARIOS"*.
Las copias de seguridad del fichero se guardaban en uno de los servidores además de en soporte CD.
PROINSSA colaboraba con uno de los centros de enseñanza secundaria de la localidad de (.....) acogiendo alumnos en prácticas. Dichos alumnos, al igual que los trabajadores de la entidad, firmaban al inicio de su actividad un compromiso de confidencialidad y custodia de la información en el que se recogía la obligación de

mantener la más estricta confidencialidad y la prohibición expresa de no realizar copias de ningún dato contenido en las bases de datos al que tuvieran acceso.
3. En el transcurso de la inspección realizada en la sede de PROINSSA, en fecha 24 de abril de 2008, se constató que el fichero aportado por la Policía Local de Ourense junto con su denuncia, coincide en su contenido con la copia de seguridad que conservaba la empresa, siendo una versión inmediatamente anterior. El representante de la entidad manifiesta desconocer la razón por la cual dicho fichero ha podido aparecer fuera del control de la entidad, toda vez que las únicas copias teóricamente existentes son las que la entidad custodia, por lo que si se ha producido un acceso o una copia indebida por parte de algún empleado o alumno en prácticas, ha sido sin su conocimiento e incumpliendo los compromisos de confidencialidad suscritos.
Se ha verificado igualmente que D. S.S.S., NIF *********, realizó prácticas de empresa en PROINSSA que comenzaron el 4 de abril de 2005, de acuerdo con la copia del compromiso de confidencialidad y custodia de la información aportada por PROINSSA suscrita por dicho alumno.
En el fichero aportado por la Policía Local de Ourense se ha localizado un registro con los datos personales de D. S.S.S., registro que no se ha localizado en el fichero en poder de PROINSSA. Entre otros datos, consta como dirección (C/.....) y como dirección de correo electrónico *"….V..@....."*.

4. El nombre, primer apellido y la dirección del titular de la dirección IP responsable de compartir el fichero en el entorno *E-mule*, en la fecha en que se localizó el mismo, coincide con la dirección, nombre y primer apellido de S.S.S., uno de los alumnos que suscribió un compromiso de confidencialidad respecto a los datos a los que tendría acceso en su condición de alumno en prácticas. Asimismo, la denominación del usuario de la red *E-mule* que compartía el fichero es *"(***V***)"* que coincide con la dirección de correo electrónico de S.S.S. *"….V.@....."*.

TERCERO: A la vista del resultado de estas actuaciones previas de investigación, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a D. S.S.S. por la presunta infracción del artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD), tipificada como leve en el artículo 44.2.e) de dicha norma.

CUARTO: El acuerdo de inicio de procedimiento sancionador fue notificado a D. S.S.S., constando la recepción por parte del interesado en fecha 30 de abril de 2008, según acuse de recibo que figura en el expediente.

QUINTO: Con fecha 2/06/08 D. S.S.S. presenta escrito de alegaciones comunicando:
<<Desde el año 2003 al año 2005 curso el Módulo de Grado Superior en Desarrollo de Aplicaciones Informáticas en el Instituto Lázaro Cárdenas de (.....). Comienzo las prácticas de ese módulo en la empresa Promoción de Iniciativas Socio-Sanitarias, en adelante PROINSSA el 4 de Abril de 2005 (...) Debido a que se me asigna la revisión del programa Gescapi en los últimos días de las prácticas, no dispongo de mucho tiempo para el mismo (...) Hubo días en los que mi trabajo no estaba terminado en la oficina y me llevé el trabajo a casa para terminarlo. En la carpeta del proyecto que me llevaba a casa se encontraba la base de datos (...) En casa poseíamos dos ordenadores de sobremesa, uno de uso familiar y el otro de uso personal mío, debido a la rotura del familiar, surgió la necesidad de compartir mi ordenador con el resto de miembros de la familia(3), de modo que pasó a ser un ordenador de uso familiar, uso que se le ha dado hasta la fecha. Por motivos de limpieza, la partición del disco duro del ordenador en la que está el sistema operativo ha sido formateada varias veces, guardando los documentos personales en otra partición. En casa usamos el programa

emule para el intercambio de archivos, este programa funciona de forma que cuanto más archivos comparte un usuario, más prioridad obtiene en sus descargas. De modo que compartimos los archivos que tenemos en la partición de los datos. De forma completamente involuntaria, y probablemente meses o incluso años después de haberme traído la base de datos a casa, fue incluida como archivo en el programa emule. Desde Octubre de 2005 a Junio de 2006 residí y trabajé en el (.....), por lo que no usé el ordenador durante ese tiempo. En mi última visita en Abril de 2006, realicé una limpieza del ordenador, formateando la partición que contenía el sistema operativo, pasando algunos archivos a la partición de datos. Creo que es en éste momento cuando copio accidentalmente los archivos pertenecientes al proyecto de gestión del aula capi, (...X.....) incluido a la partición de datos, en la que se encuentran las carpetas compartidas en el emule. En Enero de 2006 adquirí un ordenador portátil, siendo éste mi ordenador de uso personal que he conservado hasta hace unos meses, cuando adquirí otro ordenador de tipo portátil para mi uso personal. Extraje el archivo (...X.....) junto con el resto de archivos del proyecto de gestión de usuario del capi con el único fin de terminar el trabajo cuanto antes posible, ante la cercanía del fin de mi periodo de prácticas (...) El archivo se compartió en el emule de forma accidental, el ordenador en el que se encontraba el archivo es un ordenador de uso familiar. Desde Octubre de 2005 mi uso del ordenador en el que se encuentra el susodicho fichero ha sido prácticamente nulo, ya que desde Octubre de 2005 a Junio 2006 residí en el (.....) y posteriormente he dispuesto de otros dos ordenadores para mi uso personal. Viendo el registro que el programa emule guarda del número de descargas realizadas de cada archivo compartido compruebo que dicho archivo fue únicamente descargado una vez, debiendo ser ésta el archivo que se aporta con las pruebas por la Policía Local de Ourense según indica el Acuerdo de Inicio de Procedimiento Sancionador. Por tanto ninguna otra persona ha adquirido copia de este archivo mediante el programa e-mule, no pudiendo haber hecho uso de los datos que contenía (...) En cualquier caso, quiero resaltar que no tuve intención en ningún momento de hacer ningún uso de los datos contenidos en (...X.....), que si bien sacarlos de la empresa fue intencionadamente, con el único fin de proseguir con mi trabajo en casa. Quiero Indicar también, que actualmente me encuentro en situación de desempleo, y no dispongo de ningún tipo de ingreso. Estoy cursando la carrera de Ingeniería Técnica en Informática de Gestión en la Facultad de Informática de la Universidad Complutense de Madrid, para la cual el MEC me ha concedido una beca...>>

SEXTO: Con fecha 21 de julio de 2008 se acuerda por la Instructora del procedimiento la apertura de un período de práctica de pruebas,

SÉPTIMO: Con fecha 29 de julio de 2008, tiene entrada escrito de D. S.S.S., reconociendo voluntariamente su responsabilidad e indicando que ha eliminado de su ordenador el fichero denominado *"(...X.....)",* encontrado en Internet por la Policía de Orense.

OCTAVO: Al haber reconocido D. S.S.S. los hechos que se le imputan, se procede a elevar al Director de la Agencia Española de Protección de Datos el expediente a los efectos de dictar resolución al respecto.

HECHOS PROBADOS

PRIMERO: La Policía Local de Ourense localizó en una red de intercambio de ficheros cliente a cliente disponible en Internet (entorno compartido *E-mule*), un fichero denominado *"(...X.....)",* que contiene datos de 1.250 alumnos de un centro que

posiblemente gestiona PROINSSA en (.....). Los datos de los alumnos se refieren a su nombre y apellidos, dirección, teléfono, fecha de nacimiento y DNI.

SEGUNDO: La entidad PROMOCIÓN DE INICIATIVAS SOCIO-SANITARIAS, S.L.L. (PROINSSA) realizó servicios de consultoría para la ASOCIACIÓN FORTE, consistentes en la puesta en marcha y gestión del Centro de Acceso Público a Internet (CAPI) ubicado en la localidad de (.....), provincia de (…….). La prestación del servicio se realizó en el periodo comprendido entre septiembre de 2002 y Julio de 2005.

TERCERO: Para facilitar la gestión del Centro, PROINSSA creó un fichero, denominado *"CAPI-USUARIOS",* con la finalidad de gestionar los datos de inscripción de los usuarios del CAPI. Dicho fichero fue inscrito en el Registro General de Protección de Datos en fecha 5 de marzo de 2003 y con el código ########.

CUARTO: El CAPI contaba con un sistema de información consistente en una red de área local con acceso a Internet en la que convivían dos servidores y una serie de ordenadores personales instalados en las aulas. Además, se contaba con un ordenador personal en la zona de recepción en el que residía la copia de trabajo del fichero *"CAPI-USUARIOS"*. Las copias de seguridad del fichero se guardaban en uno de los servidores además de en soporte CD.

QUINTO: PROINSSA colaboraba con uno de los centros de enseñanza secundaria de la localidad de (.....) acogiendo alumnos en prácticas. Dichos alumnos, al igual que los trabajadores de la entidad, firmaban al inicio de su actividad un compromiso de confidencialidad y custodia de la información en el que se recogía la obligación de mantener la más estricta confidencialidad y la prohibición expresa de no realizar copias de ningún dato contenido en las bases de datos al que tuvieran acceso.

SEXTO: El fichero denominado *"(...X.....)",* localizado por la Policía Local de Ourense, es compartido por un usuario denominado *"(***V***)"* con dirección IP ##########.

SÉPTIMO: La dirección IP responsable de compartir el fichero en la fecha señalada tenía como titular en el momento de la localización del fichero a D. S.S.S., domiciliado en (C/.....).

OCTAVO: El fichero aportado por la Policía Local de Ourense coincide en su contenido con la copia de seguridad que conservaba la PROINSSA, siendo una versión inmediatamente anterior.

NOVENO: D. S.S.S., NIF *********, realizó prácticas de empresa en PROINSSA que comenzaron el 4 de abril de 2005, de acuerdo con la copia del compromiso de confidencialidad y custodia de la información aportada por PROINSSA suscrita por dicho alumno.

DÉCIMO: En el fichero aportado por la Policía Local de Ourense se ha localizado un registro con los datos personales de D. S.S.S., registro que no se ha localizado en el fichero en poder de PROINSSA. Entre otros datos, consta como dirección (C/.....) y como dirección de correo electrónico *"….V..@....."*.

UNDÉCIMO: El nombre, primer apellido y la dirección del titular de la dirección IP responsable de compartir el fichero en el entorno *E-mule*, en la fecha en que se localizó el mismo, coincide con la dirección, nombre y primer apellido de S.S.S., uno de los alumnos que suscribió un compromiso de confidencialidad respecto a los datos

a los que tendría acceso en su condición de alumno en prácticas. Asimismo, la denominación del usuario de la red *E-mule* que compartía el fichero es *"(***V***)"* que coincide con la dirección de correo electrónico de S.S.S. *"….V.@....."*.

DUODÉCIMO: D. S.S.S., ha comunicado que el citado fichero ha sido eliminado de su ordenador.

FUNDAMENTOS DE DERECHO

I

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

II

El artículo 8.1 del Real Decreto 1398/93, de 4 de agosto, por el que se aprueba el Reglamento del procedimiento para el ejercicio de la potestad sancionadora, dispone: *"Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento, con la imposición de la sanción que proceda."*

En aplicación del anterior precepto y teniendo en cuenta que D. S.S.S. ha reconocido los hechos imputados, procede resolver el procedimiento iniciado.

III

El artículo 10 de la LOPD dispone: *"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 confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática, a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, y, por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.
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 Constitución Española. En efecto, este precepto contiene un *"instituto de garantía 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"* (Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de

control sobre sus datos personales, sobre su uso y destino 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.
En el caso que nos ocupa, ha quedado acreditado que, empleando el programa *"eMule"*, se podía acceder sin restricción a través de Internet al fichero denominado *"(...X.....)",* que contienen datos de carácter personal relativos a 1.250 alumnos de PROINSSA, y que este fichero compartido con otros usuarios de la red se encontraba compartido por un usuario denominado *"(***V***)"* con dirección IP ##########, siendo el titular de dicha dirección IP en el momento de la localización del fichero D. S.S.S., domiciliado en (C/.....).
Asimismo ha quedado acreditado que D. S.S.S., con domicilio en (C/.....) y con dirección de correo electrónico *"…V.@....."* realizó prácticas en PROINSSA y suscribió un documento de confidencialidad y custodia de la información a la que tenía acceso durante la duración de sus prácticas, entre ellas el fichero de alumnos *"(...X.....)".*
En este caso, tal y como se ha argumentado anteriormente partiendo de unos hechos plenamente probados, se comprueba que el nombre, primer apellido y la dirección del titular de la dirección IP responsable de compartir el fichero *"(...X.....)",* en el entorno *E-mule*, en la fecha en que se localizó el mismo, coincide con la dirección, nombre y primer apellido de D. S.S.S., uno de los alumnos en prácticas que suscribió un compromiso de confidencialidad respecto a los datos a los que tendría acceso en su condición de alumno en prácticas.
También hay que tener en cuenta que la denominación del usuario de la red *Emule* que compartía el fichero es *"(***V***)"* coincide con la dirección de correo electrónico de S.S.S. *"….V.@....."*.
Por todo ello, debemos concluir que ha quedado acreditado que D. S.S.S. incumplió con el deber de secreto al que se había comprometido con PROINSSA, incurriendo así en la infracción del artículo 10 de la LOPD.

IV

El artículo 44.2.e) de la LOPD califica como infracción leve: *"Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave."*
En el presente caso, ha quedado acreditado que los datos personales que se pusieron a disposición de terceros no autorizados, a través de una red de intercambio de ficheros cliente a cliente, se trataba de datos de nombre y apellidos, dirección, teléfono, fecha de nacimiento y DNI de alumnos.
La LOPD establece cuándo la vulneración del deber de secreto del artículo 10 debe considerarse grave o muy grave, atendiendo al tipo de datos de carácter personal que han sido objeto de dicha infracción. Dado que los datos relativos a los alumnos de PROINSSSA no se encuentran en la regulación específica de grave o muy grave, procede calificar la misma como leve en virtud del trascrito artículo 44.3.e).

V

No obstante el artículo 43.1 de la LOPD, establece que: *"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."*

VI

En el presente caso, alega D. S.S.S. en su defensa que en su actuación está ausente todo elemento de culpabilidad, indispensable para que quepa apreciar la existencia de una infracción administrativa en la misma.

A este respecto, debe considerarse lo dispuesto en 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 (en lo sucesivo LRJPAC), según el cual *"... sólo 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, pues la doctrina del Tribunal Constitucional (Sentencias de 26/04/1990, 19/12/1991 y 04/07/1999, entre otras) y la jurisprudencia mayoritaria del Tribunal Supremo (Sentencia de 23/01/1998, entre otras), así como las exigencias inherentes a un Estado de Derecho, exigen que el principio de culpabilidad requiera la existencia de dolo o culpa.
El Tribunal Supremo (Sentencias de 16 y 22/04/1991) 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."*
Por su parte, la Audiencia Nacional, en Sentencia de 29/06/2001, 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...".*
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. Diligencia cuyo grado de exigencia se determinará en atención a las circunstancias concurrentes, tales como el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor. En este sentido la Sentencia de 05/06/1998 exige a los profesionales del sector *"... un deber de conocer especialmente las normas aplicables".* En similares términos se pronuncian las Sentencias de 17/12/1997, 11/03/1998, 02/03 y 17/09/1999.
Aplicando la anterior doctrina, la Audiencia Nacional, en varias sentencias, entre otras las de fechas 14/02/ y 20/09/2002 y 13/04/2005, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.
No obstante en el presente caso, ha que tenerse en cuenta que D. S.S.S., no era en origen el responsable o encargado del fichero, y teniendo en cuenta los hechos acreditados y las alegaciones del mismo, en el sentido de que ha eliminado de su ordenador el fichero denominado *"(...X.....)",* cuanto tuvo conocimiento de los hechos producidos, a través de la Agencia Española de Protección de Datos, procedería apreciar la falta de culpabilidad, tal como se recoge en la Sentencia de la Audiencia Nacional de 6 de febrero de 2008, que en su Fundamento de Derecho cuarto, establece:
<< La exigencia de la culpabilidad procede de lo que señala el artículo 130 de la Ley 30/92 cuando dice que: "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".
Por lo que se refiere a la aplicación de dicho principio de culpabilidad, hay que señalar (siguiendo el criterio de esta Sala en otras sentencias como la de fecha 21 de enero de 2004 dictada en el recurso 1139/2001) que la comisión de la infracción ' prevista en el artículo 44.3.d) puede ser tanto dolosa como culposa. Y en este sentido, si el error es muestra de una falta de diligencia, el tipo es aplicable, pues aunque en materia

sancionadora rige el principio de culpabilidad, como se infiere de la simple lectura del Art. 130 de la Ley 30/1992, lo cierto es que la expresión "simple inobservancia" del Art. 130.1 de la Ley 30/1992, permite la imposición de la sanción, sin duda en supuestos dolosos, y asimismo en supuestos culposos, bastando la inobservancia del deber de cuidado. Como ya se ha referido, la delicada materia a la que se refiere la Ley de Protección de Datos, se traduce en la necesidad de exigir una especial diligencia a las entidades gestoras de los datos. Por lo tanto, la conducta que configura el ilícito administrativo -artículo 44.3.d) de la Ley Orgánica 15/1999- requiere la existencia de culpa, que se concreta, según la resolución impugnada, en la falta de control de la entidad recurrente en comprobar si contaba con el consentimiento de la denunciante para el tratamiento de sus datos. Esa falta diligencia configura el elemento culpabilístico de la infracción administrativa y resulta imputable a la recurrente, y, obviamente, no precisa de la concurrencia de dolo.
A estos razonamientos aun cabe añadir que en nuestras Sentencias de 23 de marzo y 16 de Junio de 2004 (recursos 435/2002 y 865/2002) también señalamos que "cuando se invoca la buena fe en el actuar, para justificar la ausencia de culpa -como se hace en el presente caso- basta con decir que esa alegación queda enervada cuando existe un deber específico de vigilancia derivado de la profesionalidad del infractor. En esta línea de tradicional reflexión, la STS de 12 de marzo de 1975 y 10 de marzo de 1978, rechazan la alegación de buena fe, cuando sobre el infractor pesan deberes de vigilancia y diligencia derivados de su condición e profesional" -SAN (1a) de 14 de septiembre de 2001 (Rec. 368/2000)-". La sentencia del Tribunal Supremo (sala Tercera) de fecha 9 de Marzo de 2005 (Rec. 3895/2002) ha dicho he relación al principio de culpabilidad que: "este principio, que se garantiza en el artículo 25 de la Constitución como principio estructural básico del Derecho Penal y del Derecho Administrativo Sancionador, según refiere el Tribunal Constitucional en la sentencia 150/1991, de 4 de julio, que limita el ejercicio del ius punendi del Estado, exige que la imposición de la sanción se sustente en la exigencia del elemento subjetivo de culpa para garantizar el principio de responsabilidad y el derecho a un procedimiento sancionador con todas las garantías (STC 129/2003, de 20 de junio)"...>>
Vistos los preceptos citados y demás de general aplicación, El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: EXONERAR de responsabilidad a **D. S.S.S.** por los hechos imputados en el presente procedimiento sancionador.

SEGUNDO: NOTIFICAR la presente resolución a **D. S.S.S.** con domicilio en (C/…….....), y a la **POLICÍA LOCAL DE OURENSE** con domicilio en C/ Victoria Kent, 1 - 32001 Ourense.

TERCERO: 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. Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso

administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Procedimiento Nº PS/00324/2008

RESOLUCIÓN: R/01023/2008
En el procedimiento sancionador **PS/00324/2008,** instruido por la Agencia Española de Protección de Datos a **D. G.G.G.**, vista la denuncia presentada por **D. D.D.D.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 18 de enero de 2008 tuvo entrada en esta Agencia un escrito de D. D.D.D. (en lo sucesivo el denunciante), en el que denunciaba que con fechas 08/01/2008 y 14/01/2008 había recibido dos "SPAM" no solicitados en su dirección de correo electrónico ..D..@....., figurando como dirección de correo remitente: ..X..@....., y de los que aporta copia incluyendo código fuente más cabeceras de los mismos.
El denunciante indica que tras llamar al número de la empresa que aparece en la página Web http://www....X../, se puso en contacto telefónico con quien le fue indicado que era el responsable de misma, D. G.G.G., para solicitarle el origen de la información de su cuenta y expresarle que nunca se había dado de alta en ningún servicio de la misma para recibir publicidad. Dicha persona le indicó que le llamaría para informarle al respecto, si bien ante la falta de respuesta y la recepción de un nuevo Spam el denunciante contactó nuevamente con dicha persona, la cual le volvió a indicar que le llamaría, aunque no lo hizó.
Asimismo, el afectado señala que la cuenta ..D..@..... es de uso exclusivamente personal, utilizando otras cuentas par darse de alta en las webs, recibir notificaciones, ficheros y "Spam".

SEGUNDO: Tras la recepción de la denuncia, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:
1) D. Con fechas 8 de enero de 2008 a las 12:51:11 horas y 14 de enero de 2008 a las 10:36:34 horas, el denunciante recibió en su dirección de correo electrónico: ..D..@....., dos correos publicitarios en los que figuraba como remitente la dirección ..X..@.....
2) Los dos correos publicitarios recibidos por el denunciante tenían el siguiente contenido:

"CURSOS GRATUITOS ON-LINE DIRIGIDOS A TRABAJADORES EN ACTIVO
**Área Ofimática:*
◦ *Word, Excel, PowerPoint, Access,* ***Más información*** *Internet* ***en:***
**Área Diseño:*
◦ *DreamWeaver, Flash, PhotoShop www....X....*
**Área Sistemas – Programación:*
◦ *JAVA, .Net, Windows 2003, Linux, ORACLE, ….*
Nota Anti-SPAM:
Este mail le ha sido remitido por alguno de los siguientes motivos:
- Usted es o ha sido en algún momento cliente nuestro.
- Nos ha solicitado de forma explícita la información contenida en este correo.
- Se encuentra usted en alguna fuente de información de dominio público, como: foros, listas, libros de firmas, etc.
- Consideramos que puede ser de su interés la información aquí contenida.
Si no desea recibir más notificaciones de este tipo envíe un mail indicándolo a la dirección ..X2..@.....
Sea tan amable de aceptar nuestras disculpas si ha recibido este mail por error."

3) Con fecha 3 de marzo de 2008, a través de Internet, en el acceso efectuado a la página web: arsys.es se comprueba que como registrante del dominio "Informa.org" figura G.G.G..
4) Con fecha 19 de marzo de 2008 se constata a través del buscador GOOGLE que "Infoforma" figura como nombre asociado a la Academia Cima, con domicilio en (C/.....).
5) La denominación de la empresa es: G.G.G., siendo "Infoforma" el nombre comercial y "Academia Cima" el Centro de enseñanza donde se imparten los cursos ofertados por "Infoforma".
6) El titular del citado dominio, D. G.G.G., responsable de citado centro, con fecha 15 de abril de 2008, remitió escrito a esta Agencia poniendo de manifiesto que:
- Que dichos correos *"tienen como único objetivo informar de la impartición de cursos totalmente gratuitos para el usuario final. Nuestra finalidad es difundir esta formación gratuita entre el mayor número posible de trabajadores en activo para que se puedan en beneficiar en su preparación en nuevas tecnologías."*
- Con relación al origen de dato ..D..@..... manifiesta: "*En estos momentos lo desconozco debido a que uno de mis trabajadores, que ya no está con nosotros, se encargó de elaborar las bases de datos de la relación con los alumnos. Supongo que su origen debe estar en alguna base de datos de uso público, en alguna recomendación de alguno de nuestros alumnos."*
- No tiene constancia de la existencia de relación contractual o de otro tipo entre el titular de la dirección de correo a la que fueron remitidos dichos envíos con INFOFORMA.
- No cuenta con acreditación documental del consentimiento del denunciante para el envío de comunicaciones comerciales, especificando *que "Si se ha remitido el email al titular de la dirección de correo "..D..@....." es porque en algún momento ha estado en contacto con nosotros, o pertenece a alguna base de datos pública."*
- Tras el primer e-mail el Sr. D.D.D. se puso en contacto telefónico con él para comunicarle que no quería recibir más información nuestra, información que fue transmitida por su parte al asesor informático y de marketing, no obstante, por un error informático a los pocos días volvió a remitírsele un segundo envío.
- Que se han tomado medidas para que el denunciante no vuelva a recibir ningún correo de INFOFORMA.

TERCERO: A la vista de los hechos expuestos, con fecha 17 de junio de 2008 el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a D. G.G.G., por la presunta infracción del artículo 21 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (en lo sucesivo LSSI), tipificada como leve en el artículo 38.4.d) de la citada norma, pudiendo ser sancionada con multa de hasta 30.000 euros, de acuerdo con el artículo 39.1.c) de la misma Ley.

CUARTO: Notificado el Acuerdo de inicio con fecha 20 de junio de 2008 y transcurrido el plazo concedido para formular alegaciones al acuerdo de inicio sin que se hayan recibido las mismas, el citado acuerdo se considera propuesta de resolución, por lo que se procede a elevar el procedimiento a la resolución del Director de la Agencia Española de Protección de Datos, en virtud de lo previsto en el artículo 13.2 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.

HECHOS PROBADOS

PRIMERO: D. D.D.D. ha denunciado la recepción de dos comunicaciones comerciales no solicitadas a través de correo electrónico, cuya copia adjunta a su escrito incluyendo código fuente más cabeceras de los mismos. (Folios 1 al 14)
SEGUNDO: Dichas comunicaciones fueron recibidas por el afectado a las 12:51:11 horas del día 8 de enero de 2008 y a las 10:36:34 horas del día 14 de enero de 2008, respectivamente, en su dirección de correo electrónico "..D..@.....", habiendo sido remitidos ambos correos publicitarios desde la dirección de correo electrónico "..X..@.....". (Folios 3 y 9)

TERCERO: El contenido de los dos correos publicitarios no solicitados que fueron recibidos por el denunciante era el siguiente: (Folios 3 al 8, 9 al 14 y 36) ***"CURSOS GRATUITOS ON-LINE DIRIGIDOS A TRABAJADORES EN ACTIVO***
**Área Ofimática:*
◦ *Word, Excel, PowerPoint, Access,* ***Más información***
Internet ***en:***
**Área Diseño:*
◦ *DreamWeaver, Flash, PhotoShop www....X....*
**Área Sistemas – Programación:*
◦ *JAVA, .Net, Windows 2003, Linux, ORACLE, ….*
Nota Anti-SPAM:
Este mail le ha sido remitido por alguno de los siguientes motivos:
- Usted es o ha sido en algún momento cliente nuestro.
- Nos ha solicitado de forma explícita la información contenida en este correo.
- Se encuentra usted en alguna fuente de información de dominio público, como: foros, listas, libros de firmas, etc.
- Consideramos que puede ser de su interés la información aquí contenida.
Si no desea recibir más notificaciones de este tipo envíe un mail indicándolo a la dirección ..X2..@.....
Sea tan amable de aceptar nuestras disculpas si ha recibido este mail por error."

CUARTO: A través de Internet, en el acceso efectuado con fecha 3 de marzo de 2008 a la página web: arsys.es, se ha comprobado que como registrante del dominio "Informa.org" figura G.G.G.. (Folio 41)

QUINTO: A través del buscador GOOGLE, con fecha 19 de marzo de 2008, se ha constatado que "Infoforma" figura como nombre asociado a la Academia Cima, con domicilio en (C/.....). (Folio 40)

SEXTO: El titular del citado dominio, D. G.G.G., comunicó mediante escrito registrado en esta Agencia con fecha 15 de abril de 2008 lo siguiente: (Folios 35 al 38)
- Que dichos correos *"tienen como único objetivo informar de la impartición de cursos totalmente gratuitos para el usuario final. Nuestra finalidad es difundir esta formación gratuita entre el mayor número posible de trabajadores en activo para que se puedan en beneficiar en su preparación en nuevas tecnologías."*
- Con relación al origen de dato ..D..@..... manifiesta: "*En estos momentos lo desconozco debido a que uno de mis trabajadores, que ya no está con nosotros, se encargó de elaborar las bases de datos de la relación con los alumnos. Supongo que su origen debe estar en alguna base de datos de uso público, en alguna recomendación de alguno de nuestros alumnos."*
- Que no tiene constancia de la existencia de relación contractual o de otro tipo entre el titular de la dirección de correo a la que fueron remitidos dichos envíos con INFOFORMA.

- Que no cuenta con acreditación documental del consentimiento del denunciante para el envío de comunicaciones comerciales, especificando *que "Si se ha remitido el email al titular de la dirección de correo "..D..@....." es porque en algún momento ha estado en contacto con nosotros, o pertenece a alguna base de datos pública."*
- Que tras el primer e-mail el Sr. D.D.D. se puso en contacto telefónico con él para comunicarle que no quería recibir más información nuestra, información que fue transmitida por su parte al asesor informático y de marketing, no obstante, por un error informático a los pocos días volvió a remitírsele un segundo envío.
- Que se han tomado medidas para que el denunciante no vuelva a recibir ningún correo de INFOFORMA.

FUNDAMENTOS DE DERECHO

I

El artículo 43.1, segundo párrafo, de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, otorga a la Agencia Española de Protección de Datos la facultad para imponer sanciones por la comisión de la infracción del artículo 21 de la citada Ley.

II

El artículo 13.2 del citado Real Decreto 1398/1993, establece: *"El acuerdo de iniciación se comunicará al instructor, con traslado de cuantas actuaciones existan al respecto, y se notificará al denunciante, en su caso, y a los interesados, entendiendo en todo caso por tal al inculpado. En la notificación se advertirá a los interesados que, de no efectuar alegaciones sobre el contenido de la iniciación del procedimiento en el plazo previsto en el artículo 16.1, la iniciación podrá ser considerada propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, con los efectos previstos en los artículos 18 y 19 del Reglamento."*

III

Actualmente se denomina *"spam"* a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por *"spam"* cualquier mensaje no solicitado y que, normalmente, tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es el correo electrónico.
Esta conducta es particularmente grave cuando se realiza en forma masiva. El envío de mensajes comerciales sin el consentimiento previo está prohibido por la legislación española, tanto por la LSSI (a consecuencia de la transposición de la Directiva 2000/31/CE, de 8 de junio) como por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).
El bajo coste de los envíos de correos electrónicos vía Internet o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades que ofrece en cuanto al volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada.
El artículo 21 de la citada LSSI establece lo siguiente:
"Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.
1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que

previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija".
Así, la LSSI, en su artículo 21.1, prohíbe de forma expresa "*el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas*". Es decir, se desautorizan las comunicaciones comerciales dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, si bien esta prohibición encuentra la excepción en el segundo párrafo del citado artículo, que autoriza el envío cuando "*el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que fueron objeto de contratación*". De este modo, el envío de comunicaciones comerciales no solicitadas, fuera del supuesto excepcional del art. 21.2 de la LSSI, puede constituir una infracción leve o grave de la LSSI.
Como ya se ha señalado en cuanto a la posible obtención ilícita de los datos del destinatario, la práctica del "*spam*" además de suponer una infracción a la LSSI, puede significar una vulneración de la legislación sobre protección de datos, ya que hay que tener en cuenta que la dirección de correo electrónico puede ser considerada como dato de carácter personal.
La Directiva sobre Privacidad en las Telecomunicaciones, de 12/07/02, (Directiva 2002/58/CE) actualmente transpuesta en la Ley 32/2003, de 3 de noviembre, General de
Telecomunicaciones, que modifica varios artículos de la LSSI, introdujo en el conjunto de la Unión Europea el principio de "*opt in*", es decir, la necesidad de contar con el consentimiento previo del destinatario para el envío de correo electrónico con fines comerciales. De este modo, cualquier envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente queda supeditado a la prestación previa del consentimiento, salvo que exista una relación contractual anterior y el sujeto no manifieste su voluntad en contra.
Por lo tanto, atendiendo al enunciado del art. 21.1 de la LSSI, resulta esencial delimitar el sentido aplicado por la citada normativa a la exigencia de consentimiento, previo y expresamente manifestado por el destinatario del mensaje, para que pueda admitirse el envío de comunicaciones publicitarias o promocionales por correo electrónico.
La repetida LSSI, que tiene por objeto, entre otras materias, la regulación del envío de las comunicaciones comerciales por vía electrónica, establece expresamente en su artículo 1.2 que las disposiciones contenidas en la misma se entenderán sin perjuicio de lo dispuesto en las normas que tengan como finalidad la protección de datos personales.
Al referirse en el Título III de la LSSI a las "*comunicaciones comerciales por vía electrónica*", el artículo 19 *"Régimen Jurídico"* de la LSSI declara igualmente aplicable la LOPD y su normativa de desarrollo, "*en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de*

ficheros de datos personales". Esta rotunda previsión legal permite afirmar que, además de lo establecido en la LSSI, serán exigibles en el tratamiento de datos personales para la realización de comunicaciones comerciales por medios electrónicos el conjunto de principios, garantías y derechos contemplados en la normativa de protección de datos de carácter personal.
Por tanto, en relación al concepto de consentimiento del destinatario para el tratamiento de sus datos con la finalidad de enviarle comunicaciones comerciales por vía electrónica, es preciso considerar lo dispuesto en la normativa de protección de datos y, en concreto, el artículo 3.h) de la LOPD que establece:
"Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".
De acuerdo con dicha definición, el consentimiento, además de previo, específico e inequívoco, deberá ser informado. Y esta información deberá ser plena y exacta acerca del tipo de tratamiento y su finalidad, con advertencia sobre el derecho a denegar o retirar el consentimiento. Esta información así configurada debe tomarse como un presupuesto necesario para otorgar validez a la manifestación de voluntad del afectado.

IV

Como ya se ha señalado, la LSSI prohíbe las comunicaciones comerciales no solicitadas, partiendo de un concepto de comunicación comercial que se califica como servicio de la sociedad de la información y que se define en su Anexo de la siguiente manera:
"f) Comunicación comercial»: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.
A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica".
Por su parte el Anexo a) de la citada LSSI reconoce como Servicios de la Sociedad de la Información, entre otros y siempre que representen una actividad económica, los envíos de comunicaciones comerciales.
De acuerdo con lo señalado, es preciso analizar el concepto de Servicios de la Sociedad de la Información para, a continuación, determinar los supuestos, recogidos en el párrafo segundo del Anexo f) de la LSSI, que no se consideran, a los efectos de esta Ley, como comunicaciones comerciales.
La LSSI en su Anexo a) define como Servicio de la Sociedad de la Información, "*todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario*". A través de dicha definición el Legislador español transpuso el concepto recogido en las Directivas 98/34/CEE, de 22 de junio, del Parlamento y del Consejo, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la Sociedad de la Información, modificada por la Directiva 98/84/CE, de 20 de noviembre, del Parlamento y del Consejo, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso. Dicha definición se refiere, tal y como se expresa en el Considerando 17 de la citada Directiva 2000/31/CE, a "*cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico para el tratamiento (incluida la comprensión digital) y el*

almacenamiento de datos, y a petición individual de un receptor de un servicio", añadiendo que estos servicios cuando "*no implica tratamiento y almacenamiento de datos no están incluidos en la presente definición*".
De acuerdo con lo señalado, el concepto de comunicaciones comercial engloba la definición recogida en el Anexo f), párrafo primero de la LSSI, es decir, ha de tratarse de todas las formas de comunicaciones destinadas a promocionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o profesional, y, además, ha de realizarse dicha comunicación en los términos que señala el Considerando 17 de la Directiva 2000/31/CE que recoge lo previsto en las citadas Directivas 98/34/CE y 98/84/CE.
De lo anterior se deduce que, cuando la comunicación comercial no reúne los requisitos que requiere el concepto de Servicios de la Sociedad de la Información, pierde el carácter de comunicación comercial. En este sentido el párrafo segundo del Anexo f) de la LSSI señala dos supuestos, que no tendrán, a los efectos de esta Ley, la consideración de comunicación comercial, por un lado, los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, y, por otro, las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

V

En el supuesto examinado, tal y como ha quedado acreditado a través de la investigación realizada, D. G.G.G. remitió en fechas 8 y 14 de enero de 2008 desde la dirección de correo "..X..@....." sendas comunicaciones publicitarias a la dirección de correo electrónico "..D..@.....", sin disponer de autorización expresa y previa del destinatario de dichas comunicaciones y sin que conste la existencia de una relación contractual anterior que justifique el envío de los dos citados mensajes, de conformidad con lo dispuesto en el artículo 21.2 de la LSSI.
En dichas comunicaciones se ofrecían cursos "on line" sobre nuevas tecnologías (Ofimática, Diseño, Sistemas-Programación)" destinados a trabajadores en activo, pretendiendo, en todo caso, con el envío de dichos mensajes despertar el interés del denunciante respecto de dicho servicio docente, el cual se prestaba por el Centro de enseñanza del que D. G.G.G. es responsable.
Atendiendo a las exigencias expresadas en relación a la prestación de consentimiento para el envío de este tipo de comunicaciones, en tanto que manifestación de voluntad específica e informada, la persona imputada no ha podido acreditar que obtuvo voluntariamente del denunciante la dirección de correo electrónico "..D..@.....", mientras que éste ha denunciado que se trataba de correos comerciales no solicitados y que la cuenta de correo en la que recibió los referidos mensajes era de uso exclusivo personal, manteniendo otras cuentas para recibir "Spam".
En consecuencia, D. G.G.G. ha incurrido en la infracción del artículo 21 de la LSSI.

VI

De conformidad con lo establecido en el artículo 38, apartados 3 y 4, de la LSSI, se consideran infracciones graves y leves las siguientes:
"3. Son infracciones graves:"
"c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo

destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21".
"4. Son infracciones leves:"
"d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave".
En consecuencia, el envío de comunicaciones comerciales no solicitadas, en los términos indicados por el citado artículo 38.4.d) de la LSSI se califica como infracción leve, con el agravante de que si se produce un envío masivo de comunicaciones comerciales no solicitadas a diferentes destinatarios o más de tres a un mismo destinatario en el plazo de un año, en los términos que se indican el también citado artículo 38.3.c), se producirá una infracción grave a los efectos de dicha Ley.
El presente supuesto se ajusta al tipo de infracción establecido en el artículo 38.4.d), calificado como infracción leve, al tratarse del envío por correo electrónico de dos comunicaciones comerciales no deseadas a un mismo destinatario en el plazo de un año.

VII

A tenor de lo establecido en el artículo 39.1.c) de la LSSI, las infracciones leves serán sancionadas con multa de hasta 30.000 euros, estableciéndose los criterios para su graduación en el artículo 40 de la misma norma, que establece lo siguiente:
"Artículo 40. Graduación de la cuantía de las sanciones.
La cuantía de las multas que se impongan se graduará atendiendo a los siguientes criterios:
a) La existencia de intencionalidad.
b) Plazo de tiempo durante el que se haya venido cometiendo la infracción.
c) La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.
d) La naturaleza y cuantía de los perjuicios causados.
e) Los beneficios obtenidos por la infracción.
f) Volumen de facturación a que afecte la infracción cometida".

En base a estos criterios y, en especial, la ausencia de reincidencia acreditada en el presente procedimiento sancionador, procede la imposición a D. G.G.G. de una sanción por importe de 600 euros.
Vistos los preceptos citados y demás de general aplicación,
El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: IMPONER a **D. G.G.G.** por una infracción del artículo 21 de la LSSI, tipificada como leve en el artículo 38.4.d) de dicha norma, una sanción de 600 € (seiscientos euros) de conformidad con lo establecido en los artículos 39.1.c) y 40 de la citada Ley.

SEGUNDO: NOTIFICAR la presente resolución a **D. G.G.G.,** con domicilio en (C/.....), y a **D. D.D.D.** con domicilio en (C/.....).

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario,

se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.
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.
Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Procedimiento Nº PS/00328/2005

RESOLUCIÓN: R/00457/2006

En el procedimiento sancionador **PS/00328/2005**, instruido por la Agencia Española de Protección de Datos a la entidad **ARCADIA INTERNACIONAL, S.A., ARVATO SERVICES IBERIA S.A.,** y **CENTRO DE ESTUDIOS CEAC S.L.**, vista la denuncia presentada por **D. J.B.S.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 05/10/2004, tuvo entrada un escrito de D. J.B.S. (en lo sucesivo el denunciante), en el que declara que ha recibido por correo postal una información comercial de la compañía ARCADIA INTERNACIONAL S.A. (en lo sucesivo Arcadia), estando en desacuerdo con el procedimiento utilizado por esta compañía para la obtención de sus datos personales.
Así mismo, manifiesta su disconformidad con el hecho de que, en la propia información comercial, Arcadia le comunique la cesión de sus datos a otras compañías en el caso de que no manifieste lo contrario.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas de investigación, por los Servicios de Inspección de esta Agencia se solicitó información a las entidades Arcadia, ARVATO SERVICES IBERIA, S.A. (en lo sucesivo Arvato) y a CENTRO DE ESTUDIOS CEAC, S.L. (en lo sucesivo Ceac), teniendo conocimiento de los siguientes extremos:
A) Los datos del denunciante figuran en las *"Páginas Blancas"* accesibles a través de Internet, sin embargo en esta publicación no consta el piso y la puerta que sí aparecen en la dirección postal a la que se dirigió el envío publicitario.
B) La compañía que figura en el envío publicitario, Arcadia, ha manifestado que los datos utilizados para el citado *"mailing",* realizado en septiembre de 2004, les fueron facilitados por Arvato según consta en el lateral de la comunicación recibida por el denunciante. En el mismo se informa que "*El listado de direcciones utilizado para la realización de esta campaña publicitaria ha sido elaborado por la entidad Arvato Services Iberia, S.A. (C/....., Teléfono ########), a la que usted puede dirigirse a fin de ejercer sus derechos de acceso, rectificación, cancelación y oposición".* Así mismo manifiesta que los datos relativos al denunciante no se han incluido en los ficheros de la entidad Arcadia dado que, al no interesarse en los productos promocionados, no llegó a ser cliente suyo. La citada relación jurídica entre Arcadia y Arvato se formalizó en el contrato, suscrito entre ambas partes con fecha 3/01/2000, por el que Arcadia le encomienda la elaboración de un listado de destinatarios de una campaña o acción publicitaria, para lo cual podrá utilizar sus propios ficheros o los de terceras personas o entidades con las que Arvato firme los correspondientes contratos de *"listbroking".* Arvato emitió por dichos servicios varias facturas a Arcadia.
C) Arvato informa que los datos utilizados para elaborar el listado de destinatarios de la campaña publicitaria de Arcadia, procedían, en parte, del fichero *"Maestro de Promociones"*, como consecuencia del contrato de *"listbroking"* que celebró el 2/12/2003 con Ceac, en virtud del cual Arvato se convertía en encargado del tratamiento de Ceac, con el fin de proceder a la distribución del citado fichero entre los clientes de Arvato.
D) Ceac ha informado que los datos relativos al denunciante se los facilitó el propio interesado el 21/11/2003, a través de su página web, en la que se incluye un *"formulario de solicitud de información"* sobre los cursos que ofrecen.

En el citado formulario remitido a la Agencia por Ceac, figura la siguiente información "*Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de Centro de Estudios CEAC, S.L. para gestionar la relación comercial con usted. Usted tiene los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía: (C/.....). Es posible que en un futuro –incluso finalizada nuestra relación comercial- utilicemos sus datos personales para informarle sobre nuestros productos y/o servicios o que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollen su actividad en los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, con el fin de que le informen sobre los productos o servicios que comercialicen*."

TERCERO: A la vista del resultado de las actuaciones previas de investigación, el Director de la Agencia Española de Protección de Datos acordó, en fecha 9/01/2006, iniciar procedimiento sancionador a las entidades Arcadia y Arvato por las presuntas infracciones del artículo 6.1 de la Ley Orgánica 15/1999, de 13/12, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), tipificadas como graves en el artículo 44.3.d) de dicha norma, pudiendo ser sancionada cada una de ellas, con multa de 60.101,21 € a 300.506,05 € , de acuerdo con el artículo 45.2 de la citada Ley Orgánica.
Igualmente, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a Ceac por la presunta infracción del artículo 11 en relación con el 5.1 de la LOPD, tipificada como muy grave en el artículo 44.4.b) de dicha norma, pudiendo ser sancionada con multa de 300.506,05 € a 601.012,10 € , de acuerdo con el artículo 45.3 de la citada Ley Orgánica.

CUARTO: Notificado el acuerdo de inicio a las citadas entidades, todas ellas formularon alegaciones en el siguiente sentido:
A) Ceac manifestó lo siguiente: *"...se aportaba copia de la página del formulario de captación de datos que, en fecha 21 de noviembre de 2003, el Sr. J.B.S. cumplimentó para solicitar información a CEAC sobre un curso de Técnico de Gestión Medioambiental".*
"La cuestión se centra, pues, en analizar si la literalidad de la Cláusula Informativa puede considerarse inequívoca, de tal manera que pueda concluirse que el denunciante dio su autorización para recibir publicidad de los concretos productos de ARCADIA..."
"... los términos de la denuncia no apuntan a una infracción por parte de CEAC de derecho alguno del denunciante, dado que ni tan siquiera menciona a esta compañía en la misma..."
"...se aprecia que la Cláusula Informativa cumple perfectamente con los requisitos del artículo 5.1..."
"...Ceac no ha infringido el artículo 5.1 de la LOPD (...), sino que tampoco le es imputable en ningún caso, la infracción del artículo 11.1 de la LOPD, dado que según la propia APD la relación entre CEAC y ARVATO SERVICES IBERIA, S.A. no es la de cedente-cesionario, sino la de titular del fichero-prestador de servicios, lo que excluye la operativa de estas dos compañías del régimen jurídico del artículo 11 de la LOPD, situándola bajo el régimen del artículo 12 de la misma."
"...CEAC ha seguido el criterio del citado Gabinete Jurídico que, por dos veces, se ha pronunciado sobre la información que el responsable del fichero debe facilitar en el momento de captación de los datos, para así respetar las normas contenidas en los propios preceptos (...)

A continuación, resulta obligada la referencia al informe que el Gabinete Jurídico de la APD emitió de forma particular a favor del GRUPO PLANETA- al que pertenece CEAC (...) el GRUPO PLANETA sometió a valoración de la APD la siguiente cláusula informativa:

<< Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de_____, S.A. para gestionar la relación comercial con usted. Usted podrá ejercer los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía Calle ,_____. Del mismo modo, Ud. consiente a que en un futuro -incluso finalizada nuestra relación comercial -_____, S.A. utilice sus datos personales para informarle sobre sus productos y/o servicios y a que comunique tales datos a otras empresas del Grupo Planeta cuyas actividades se relacionen con los sectores editorial, de formación, de cultura y de ocio, con el fin de que le informen sobre los productos o servicios que comercialicen. Si no desea ser informado de nuestros productos o servicios o de los de otras empresas del Grupo Planeta, indíquenoslo por escrito en la dirección arriba indicada, señalando claramente su nombre, apellidos y dirección o hágalo constar en este cupón, marcando la siguiente casilla □ (Ley Orgánica 15/1999 de 13 de Diciembre).>>"

"La anterior argumentación en cuanto a la "confianza legítima" creada por la APD debe extenderse a la doctrina que emana de todas las resoluciones de la APD a que se ha hechos mención a lo largo de este escrito."

B) Igualmente, Arcadia presentó escrito de alegaciones, en el que comunica entre otros extremos:

"El denunciante prestó a Ceac su consentimiento para la recepción de publicidad de los productos promocionados por Arcadia (...) si este aspecto queda despejado en sentido afirmativo, está claro que ARCADIA deberá ser liberada de cualquier responsabilidad."

"...ARCADIA ocupa en este caso la posición de beneficiario de la publicidad, según así lo acredita el contrato suscrito con ARVATO (...) en fecha 3 de enero de 2000, por el que esta última compañía declara que se dedica a la recopilación de direcciones, prospección comercial (...) y, por ello, tiene suscritos contratos con titulares de ficheros para elaborar listados de direcciones para terceros beneficiarios de la publicidad, como lo es ARCADIA."

"...tratándose de supuestos idénticos, porque intervino una empresa listbroker, como agente del titular del fichero, la APD ni si quiera incoó procedimiento sancionador contra el beneficiario de la publicidad..."

C) Asimismo, Arvato presentó escrito de alegaciones, en el que comunica:

"...resulta evidente que la imputación a ARVATO SERVICES IBERIA, S.A. de la realización de un tratamiento o uso de datos de carácter personal, por lo que se refiere al afectado señor J.B.S. , supuestamente conculcando "los principios y garantías" establecidos en la Ley Orgánica de Protección de Datos de Carácter Personal (en este caso según se indica 1o dispuesto en su artículo 6: el consentimiento del afectado), supone obviar un elemento fundamental, y que ha quedado perfectamente recogido y acreditado en las actuaciones, el de que mi representada se ha limitado a actuar, en todo momento, por cuenta de la entidad responsable del fichero, en este caso CENTRO DE ESTUDIOS CEAC, S.L. procediendo, en base a la documentación contractual suscrita con la misma, a actuar como su Agente comercial en orden a promover la utilización de direcciones de personas que figuran en sus ficheros de datos de carácter personal, en la realización de acciones publicitarias de terceras empresas o entidades (en el caso concreto que nos ocupa ARCADIA), así como a elaborar dichos listados, en su condición de empresa especializada en la realización de acciones de marketing y publicidad directa, siempre contando, a tales efectos, con la previa conformidad de dicha entidad titular para ello y cumplimentando, en el

desarrollo y realización de todo ello, las normas legales de obligada observancia y, en especial, cuanto viene requerido en la normativa sobre protección de datos de carácter personal la cual, insistimos, en momento alguno ha sido conculcada por ARVATO..."
"...en ningún caso ha efectuado o llevado a cabo, respecto de los datos del afectado (...), tratamiento alguno sin contar con la previa y expresa autorización y conformidad de la entidad titular del fichero en el que figuran recogidos los mismos, habiendo actuado, por lo demás y en todo momento respecto de los trabajos realizados en orden a la elaboración de los listados de destinatarios de envíos publicitarios de terceras entidades, con plena sujeción a los requisitos contractuales establecidos por la entidad titular del fichero los cuales, igualmente, y tanto en su dicción como en su operativa material posterior, se ajustan plenamente a los exigidos en el artículo 12 de la Ley Orgánica de Protección de Datos de Carácter Personal."
"...no cabe pueda imputársele responsabilidad sobre un extremo: la concurrencia del consentimiento del afectado en orden a poder ser incluido en un listado de destinatarios de un envío de carácter publicitario, en tanto en cuanto ello, obviamente, incumbe, exclusivamente, al responsable del fichero, es decir, en este caso: CENTRO DE ESTUDIOS CEAC, S.L.,"
"...mi representada se ha ajustado, en todo momento y en su actuar, a las instrucciones y autorizaciones de la entidad responsable del fichero queda asimismo acreditada, en relación con la operativa seguida para la realización del envío publicitario origen de las presente actuaciones, de la comprobación del contenido del contrato que, a su vez, mi mandante suscribió con la entidad beneficiaria de la publicidad (en este caso la entidad Arcadia Internacional, S.A.) bastando proceder a su revisión para constatar, como se ha indicado, que en momento alguno dicha entidad beneficiaria puede disponer en modo o forma alguna de los datos personales del afectado salvo que, como informó la misma a esa Agencia, dicho afectado pueda aceptar la oferta y, en tal caso, contacte éste directamente con Arcadia..."
"Por otro lado, y del contenido del mencionado contrato suscrito entre mi representada y la entidad Arcadia, así como de las demás documentación re1acionada con la campaña o acción publicitaria que nos ocupa..."
"...en ningún caso puede derivarse, de la eventual falta de concurrencia del consentimiento del afectado para recibir publicidad de terceras entidades, responsabilidad alguna para mi mandante o la entidad beneficiaria de la acción publicitaria, ya que ello, insistimos, es un requisito que debe ser observado y cumplido por la entidad titular del fichero (...) mi mandante, en orden a mantener la máxima diligencia en la observancia de cuanto se dispone en la normativa de protección de datos de carácter personal, recabó, en su momento, la expresa y formal declaración y confirmación, por parte de la entidad titular del fichero en que figuraban los datos utilizados para la remisión del envío publicitario origen de las presentes actuaciones, tanto del debido registro y notificación del propio fichero como respecto de la concurrencia del consentimiento de las personas incluidas en el mismo al efecto de que sus datos pudieran ser incluidos en listados de destinatarios de campañas publicitarias de terceras entidades..."

QUINTO: Durante la fase de práctica de pruebas, se solicitó al denunciante que remitiera a esta Agencia Española de Protección de Datos, el envío publicitario completo recibido de Arcadia, sin que atendiera dicha solicitud.

SEXTO: Terminada la fase de pruebas, se inició el trámite de audiencia en que el expediente se puso de manifiesto a las entidades imputadas, que presentaron nuevos escritos de alegaciones, ratificándose en las manifestadas al acuerdo de inicio, y comunicando Arcadia lo siguiente:

"*El aspecto de vital importancia en la defensa de los intereses de ARCADIA es el de la calificación de la operativa seguida con ARVATO (...) según la propia opinión de la APD. Porque según esta última Administración la relación entre el titular del fichero y el "list-broker" se enmarca en el régimen jurídico del artículo 12 de la LOPD, lo que conlleva la ausencia de responsabilidad del "list-broker" y mucho menos del beneficiario de la publicidad*."

SÉPTIMO: Con fecha 5/06/2006 se emitió propuesta de resolución, en el sentido de que por el Director de la Agencia Española de Protección de Datos se sancionase a las entidades Arcadia y Arvato con multa de 60.101,21 €, a cada una de ellas, por las infracciones del artículo 6.1 de la LOPD, tipificadas como graves en el artículo 44.3.d) de dicha norma, así como a la entidad Ceac con multa de 300.506,05 €, por la infracción del artículo 11 de la LOPD, tipificada como muy grave en el artículo 44.4.b) de dicha norma.

OCTAVO: Con fecha 3/07/2006, tuvieron entrada en esta Agencia las alegaciones de Arcadia, frente a la propuesta de resolución, en las que después de razonar que existe una ausencia de culpa en su conducta, solicita la aplicación del artículo 45.5 de la LOPD, por una cualificada disminución de la culpabilidad en su actuación por cuanto la citada entidad actuó creyendo que si nunca trató los datos del denunciante no podría producirse una vulneración del art. 6 de la LOPD.
También con fecha 3/07/2006, tuvieron entrada en esta Agencia las alegaciones formuladas por Arvato, en las que insiste que ha actuado, en todo caso, como un mero encargado de tratamiento en su condición de agente comercial de Ceac, siguiendo las instrucciones de ésta de acuerdo con el contrato de "*listbroking*" suscrito entre ambas el 2/12/2003. Por tanto, no ha efectuado tratamiento alguno sin contar con la previa y expresa autorización de Ceac, siendo ésta la única entidad que decide, en todo momento, sobre los usos y finalidades de su fichero sin mediatización o condicionante de ninguna clase. Por ello concluye que "*en modo alguno cabe imputar … la infracción de ninguna clase, ya que ésta en ningún momento ha adoptado decisión alguna respecto del fichero de Ceac habiéndose limitado al mero cumplimiento de lo dispuesto en el oportuno contrato suscrito por ambas entidades de conformidad con lo dispuesto en el artículo 12 de la LOPD…*".
Con fecha 4/07/2006, Ceac formuló alegaciones a la propuesta de resolución en las que, básicamente, señalaba su disconformidad con la imputación realizada en la misma en base a los siguientes argumentos:
1. Ceac obtuvo del denunciante su consentimiento inequívoco en base a la cláusula informativa que implementó en la recogida de los datos a través de su página web, argumentando que esta Agencia se separa en la propuesta de las recomendaciones dictadas en 2001, 2003 y 2004 por cuanto en las mismas, se señalaba como suficiente la referencia a sectores de actividad, resultando por ello a su juicio, desvanecida la confianza legítima creada por la propia Agencia. Por ello considera que, si de la citada cláusula no se derivara el consentimiento inequívoco del denunciante en la propuesta, se estaría asimilando a Ceac con el supuesto de un responsable de un fichero que recaba datos sin inclusión de cláusula informativa alguna.
2. Que Ceac actuó como responsable del fichero y Arvato como su encargado en virtud del contrato suscrito entre ambas con fecha 2/12/2003, ya que la entrega del fichero tiene carácter instrumental en orden al cumplimiento de las obligaciones del agente (Arvato) que actuará bajo la autorización y tutela de Ceac.
3. Solicita la aplicación del art. 45.5 de la LOPD porque, básicamente, siempre creyó que la cláusula informativa cumplía con las previsiones de la LOPD, y porque ha variado la cláusula informativa en los términos en que se informó por el Gabinete Jurídico de esta Agencia.

HECHOS PROBADOS

PRIMERO: Los datos de D. J.B.S. figuran en las *"Páginas Blancas"*, accesibles a través de Internet, sin embargo en esta publicación no consta el piso y la puerta que sí aparecen en la dirección postal a la que se dirigió el envío publicitario de Arcadia (folio 7).

SEGUNDO: D. J.B.S. facilitó, en fecha 21/11/2003, a Ceac sus datos personales, al solicitar información sobre un curso de Técnico de Gestión Medioambiental, a través de su página web, en la que se incluye *un "formulario de solicitud de información"* sobre los cursos que ofrecen.
En el citado formulario de recogida de datos de Ceac, figuraba la siguiente información *"Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de Centro de Estudios CEAC, S.L. para gestionar la relación comercial con usted. Usted tiene los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía: (C/.....). Es posible que en un futuro –incluso finalizada nuestra relación comercial- utilicemos sus datos personales para informarle sobre nuestros productos y/o servicios o que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollen su actividad en los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, con el fin de que le informen sobre los productos o servicios que comercialicen*" (folio 213). El subrayado recoge el contenido de la cláusula que difiere de la sometida a informe del Gabinete Jurídico de la Agencia, que se recoge en el Hecho Probado Sexto que más adelante se transcribe.

TERCERO: En septiembre de 2004, D. J.B.S. recibió por correo postal una información comercial de la compañía Arcadia, estando en desacuerdo con el procedimiento utilizado por esta compañía para obtener sus datos personales. En el mismo se informa que "*El listado de direcciones utilizado para la realización de esta campaña publicitaria ha sido elaborado por la entidad Arvato Services Iberia, S.A. (C/....., Teléfono ########), a la que usted puede dirigirse a fin de ejercer sus derechos de acceso, rectificación, cancelación y oposición"*, previsto para los casos en los que los datos no procedan del *"fichero BDT"* cuyo responsable es Arvato (folios 1 a 4).

CUARTO: La compañía que figura en el envío publicitario, Arcadia, ha manifestado que los datos utilizados para el citado *"mailing",* realizado en septiembre de 2004, les fueron facilitados por Arvato según consta en el lateral de la comunicación recibida por el denunciante, cuyo tenor literal se ha recogido en el Hecho Probado anterior. Asimismo, manifiesta que los datos relativos al denunciante no se han incluido en los ficheros de la entidad Arcadia, dado que, al no interesarse en los productos promocionados, no llegó a ser cliente suyo. Arvato y Arcadia suscribieron un contrato el 3/01/2000, por el que aquélla encomienda a Arvato la elaboración de un listado de destinatarios o de una campaña o acción publicitaria, para lo cual podrá utilizar sus propios ficheros o los de terceras personas o entidades con las que Arvato firme contratos de *"listbroking".*
Arvato ha remitido diversas facturas emitidas por los servicios que presta a Arcadia (folios 11- 12, 31 – 38, 42 - 44, 39 - 41). En las diversas facturas, remitidas por Arvato a esta Agencia Española de Protección de Datos en relación con los servicios prestados por la misma a la entidad Arcadia, consta claramente que es esta entidad,

Arvato, quien realiza la facturación y el cobro de los servicios prestados, haciendo sólo en la descripción, una referencia a los ficheros de los que se han obtenido los datos.

QUINTO: En el contrato de 2/12/2003, suscrito entre Arvato y Ceac, se informa que los datos utilizados para elaborar el listado de destinatarios de la campaña publicitaria de Arcadia, recibida por el denunciante, proceden del fichero que le facilitó la entidad Ceac, con quien ha suscrito el citado contrato de *"listbroking*".
En el citado contrato, apartado II, se manifiesta que *"ARVATO dispone, para su actividad, de los más variados contactos con empresas para las que desarrolla campañas de publicidad directa mediante el tratamiento automatizado de listas de nombres...A los efectos de este contrato, tales empresas se referirán como los <<CLIENTES>>"* (folio 47).
A lo largo del texto del citado contrato, apartado V, se establece lo siguiente:
"Que, con independencia de los acuerdos o pactos que ARVATO pueda tener establecidos con"...(en este caso, Ceac)...*"de forma previa a su tratamiento y utilización para cualquier campaña encargada por un CLIENTE..."* (en este caso, Arcadia)..."*procede a recabar la oportuna aprobación por escrito del TITULAR DEL FICHERO"*...(en este caso, Ceac)..."*respecto del encargo de que, en cada caso, se trate"* (folio 48).
El TITULAR DEL FICHERO ...(en este caso, Ceac*)..."manifiesta que ha recabado el consentimiento de las personas cuyos datos personales obran en el fichero"*...(en este caso el *"Fichero Maestro de Promociones"*, de Ceac)..."*para que sus datos personales sean utilizados para fines publicitarios por empresas que desarrollan su actividad en los sectores de telecomunicaciones, financiero, ocio, formación, gran consumo, automoción, energía, agua, y ONG"* (pacto primero, párrafo tercero del mencionado contrato) (folio 49).
"ARVATO está autorizada para representar al TITULAR DEL FICHERO"...(en este caso Ceac)..."*en la negociación de los contratos con los CLIENTES"...*(en este caso, con Arcadia*)..."A estos efectos, actuará en nombre y por cuenta del TITULAR DEL FICHERO"* (Ceac), (pacto segundo del contrato) (folio 50).
"*Con la firma de este contrato el TITULAR DEL FICHERO"*...(en este caso, Ceac)..."*facilita a ARVATO una copia completa y actualizada del fichero"*...(en este caso *"Fichero Maestro de Promociones"*..."*en soporte informático para su más ágil tratamiento en las instalaciones de ARVATO"*..."*la entrega del mismo tiene un mero carácter instrumental...sin que ello suponga, en ningún caso, ...alteración ...ni modificación de carácter del TITULAR DEL FICHERO o su responsabilidad sobre el fichero*" (pacto cuarto, párrafos primero y segundo) (folio 50).
"EL TITULAR DEL FICHERO percibirá las contraprestaciones que se fijen..." "ARVATO percibirá por los servicios prestados al TITULAR DEL FICHERO las contraprestaciones indicadas en el anexo..." (pacto séptimo del citado contrato) (folio 52).
Por lo que se refiere a las *"condiciones económicas*", de "*facturación y pago*" y de "*contraprestaciones del Agente*", el Anexo al contrato de 2/12/2003 dispone que Ceac, como TITULAR DEL FICHERO, percibirá las contraprestaciones en función de la utilización de las direcciones realizada por ARVATO, expidiendo la correspondiente factura a la fecha de confirmación que le haga ARVATO que, como agente, percibirá una comisión que se deducirá de la factura expedida por Ceac (Anexo al contrato en folios 56-58).

SEXTO: El Grupo Planeta, al que pertenece Ceac, sometió a informe del Gabinete Jurídico de la Agencia Española de Protección de Datos, la siguiente cláusula informativa que difiere de la implementada por la citada entidad, en este caso, para la recogida de datos del denunciante. Dicha cláusula tenía el siguiente tenor literal:

<< Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de_____, S.A. para gestionar la relación comercial con usted. Usted podrá ejercer los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía Calle ,_____. Del mismo modo, Ud. consiente a que en un futuro -incluso finalizada nuestra relación comercial -_____, S.A. utilice sus datos personales para informarle sobre sus productos y/o servicios y a que comunique tales datos a otras empresas del Grupo Planeta cuyas actividades se relacionen con los sectores editorial, de formación, de cultura y de ocio, con el fin de que le informen sobre los productos o servicios que comercialicen. Si no desea ser informado de nuestros productos o servicios o de los de otras empresas del Grupo Planeta, indíquenoslo por escrito en la dirección arriba indicada, señalando claramente su nombre, apellidos y dirección o hágalo constar en este cupón, marcando la siguiente casilla □ (Ley Orgánica 15/1999 de 13 de Diciembre).>>" (folio 193).

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

De los antecedentes y hechos probados señalados con anterioridad, se deducen dos cuestiones de fondo. La primera, si cabe deducir que Ceac obtuvo, en el momento de la recogida de los datos, a través del formulario incluido en su página web, el consentimiento inequívoco del denunciante de modo que se encontrara habilitada para su cesión a terceros sin consentimiento del mismo, y, la segunda, si la entidad Arvato ha actuado en el presente supuesto como encargado de tratamiento de Ceac, en virtud del contrato suscrito por ambas entidades el 2/12/2003.

III

Respecto a la primera cuestión el artículo 5 de la LOPD, dispone lo siguiente:
"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos
. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten."
De acuerdo con lo establecido en el citado artículo 5 de la LOPD, el responsable del fichero debe informar, en el momento de la recogida de los datos, de los extremos establecidos en el citado artículo. La información a la que se refiere el citado artículo debe suministrarse a los afectados previamente a la recogida de sus datos personales, y deberá ser expresa, precisa e inequívoca.
El número 2 del mismo precepto establece una regla especial para los supuestos en que se utilicen cuestionarios u otros impresos para la recogida de los datos, exigiendo que *"figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior."*
La LOPD ha querido, por tanto, imponer una formalidad específica en la recogida de datos a través de cuestionarios u otros impresos, que garantice el derecho a la información de los afectados. A tal efecto, impone la obligación de que la información figure en los propios cuestionarios o impresos, y la refuerza exigiendo que conste de forma claramente legible.

IV

La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que delimita el contenido esencial del derecho fundamental a la protección de los datos personales, se ha pronunciado sobre la importante vinculación entre el consentimiento y la finalidad para el tratamiento de los datos personales, en los siguientes términos: *" el derecho a consentir la recogida y el tratamiento de los datos personales (art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con éstos (art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por*

tanto, esté justificada, sea proporcionada y, además, se establezca por ley, pues el derecho fundamental a la protección de datos personales no admite otros límites.
De otro lado, es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia" (el subrayado es de la Agencia Española de Protección de Datos).
De lo expuesto cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales en lo relativo a los requisitos del consentimiento, de la información previa a éste, y de las finalidades para las que los datos pueden ser recabados y tratados.
Asimismo, la citada Sentencia 292/2000, ha considerado el derecho de información como un elemento indispensable del derecho fundamental a la protección de datos al declarar que *"el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.*
En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele." (el subrayado es de la Agencia Española de Protección de Datos).

V

Ceac en las alegaciones a la propuesta de resolución señala que la cláusula informativa que implementó en la página web, en el momento de la recogida de los datos, es suficiente para acreditar un consentimiento inequívoco del denunciante, haciendo referencia a que esta Agencia siempre ha entendido suficiente la enumeración de los sectores de actividad a los cuales se haría cesión de los datos.

Frente a dicha alegación, ha quedado acreditado en el presente procedimiento sancionador, y así ha sido reconocido por Ceac, que dicha entidad se separó del informe emitido por el Gabinete Jurídico de esta Agencia, señalando que nunca ha defendido la identidad de leyendas, sino la identidad de criterios contenidos en ambas leyendas. Dicha alegación no puede ser compartida por esta Agencia ya que la cláusula finalmente aplicada por Ceac recogía diferencias sustanciales de las cuales se deducía la recogida de un consentimiento no inequívoco por parte de los interesados.

De acuerdo con lo señalado, en el presente caso, consta acreditado que Ceac ha venido utilizando una cláusula informativa, en el momento de la recogida de los datos a través de su web, que no recoge los extremos a que se refiere el apartado a) del artículo 5.1 de la LOPD, sin que de dicha información se dedujese claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que éstos se recaban.

En relación al citado apartado a) del artículo 5.1, la citada cláusula informativa no concreta de modo expreso, preciso e inequívoco la finalidad de la recogida de los datos y de los destinatarios de la información, ya que las referencias a *"los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones",* se refiere a términos inconcretos de los que no caben deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos, lo que impide que el interesado pueda conocer, como señala el Tribunal Constitucional, *"a qué uso lo está destinando y , por otro lado, el poder oponerse a esa posesión y usos".*

En este sentido, resultan ejemplificadores dos circunstancias que han concurrido en el presente supuesto:

-- El propio denunciante, que según Ceac había prestado un consentimiento informado, a través de su web al solicitar información sobre un curso el 21/11/2003, sin embargo no pudo asociar que el envío publicitario de Arcadia, en el que se le informaba que el listado de direcciones había sido elaborado por Arvato, sobre el *"Fichero Maestro de Promociones"* de Ceac, tuviera ninguna relación con la citada recogida de datos.

-- Ceac en el formulario de recogida de datos se refiere a la comunicación a empresas de los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, cuando en el contrato suscrito con Arvato el 2/12/2003 se refiere a los sectores de las telecomunicaciones, financiero, ocio, formación, gran consumo, energía, agua y ONG, existiendo una clara diferencia en cuanto a que en el contrato de 2/12/2003, no se prevé que Ceac le pueda dar acceso a Arvato para fines de venta por correo y/o comunicaciones. Frente a dicha argumentación Ceac señala en las alegaciones a la propuesta que de dicha discordancia no se aprecia qué consecuencia jurídica puede ello acarrear en cuanto a los derechos del denunciante, ya que la relación entre Ceac y Arvato es bilateral y privada, y lo importante no es el contenido de dicha relación sino el de la cláusula informativa que reciba. No puede admitirse dicha alegación, porque el consentimiento inequívoco del denunciante, sobre el que se fundamenta el poder de control y disposición de sus datos, es el que debe limitar los usos y finalidades que, precisamente, pretendan realizarse con los mismos.

A mayor abundamiento, la Audiencia Nacional en Sentencia de 13/04/2005 ya señaló que *"la amplitud de categoría de bienes y servios para los que se presta el consentimiento... tampoco permite al particular, identificar de forma determinada y explícita las finalidades para los que serán tratados sus datos personales, en términos que le permitan prestar un conocimiento inequívoco como el exigido por la LOPD".*

Tampoco en la cláusula informativa se informa de modo expreso, preciso e inequívoco, sobre los destinatarios de la información, haciéndose una genérica referencia en el siguiente sentido "...*que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo..."* En este sentido, como más

adelante se referirá, la cláusula informativa de Ceac no coincide con la informada por esta Agencia con fecha 7/07/2004, ya que añade de forma inconcreta los destinatarios de los datos al referirlos, en general, a *"empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo".*
De acuerdo con lo señalado, de la cláusula implementada por Ceac no cabe deducir que el denunciante hubiese prestado su consentimiento inequívoco para el tratamiento de sus datos, y , menos aún, para proceder a ceder sus datos a un tercero. Por lo tanto se considera que Ceac ha vulnerado lo previsto en el artículo 11 de la LOPD, que en su apartado 1, dispone lo siguiente:
"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."
En el supuesto examinado, ha quedado probado que la entidad Ceac es la responsable del *"Fichero Maestro de Promociones"* del que se obtuvieron los datos del denunciante utilizados para el envío publicitario enviado, sin que haya acreditado que tuviera el consentimiento del denunciante para comunicar sus datos a Arvato, ni estar exceptuada para ello conforme al apartado 2 de dicho precepto.

VI

El artículo 44.4.b) de la LOPD, establece que será infracción muy grave:
" b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas".
En el presente caso, ha quedado acreditado que Ceac comunicó los datos del denunciante a Arvato sin que constara el consentimiento inequívoco de éste ya que los términos recogidos en la cláusula informativa, recogida en la web de Ceac, no incluía los extremos a los que se refiere el apartado a) del artículo 5 de la LOPD. En consecuencia, la citada comunicación supone una vulneración del artículo 11 de la LOPD que encuentra su tipificación en el citado artículo 44.4.b) la citada Ley Orgánica.

VII

En cuanto a la segunda cuestión de fondo que se planteaba en el Fundamento de Derecho I de esta Resolución, es decir sobre si, en el presente supuesto, Arvato ha actuado como encargado de tratamiento de Ceac, al amparo del contrato suscrito entre ambas entidades el 2/12/2003, en cuyo caso no debería responder de vulneración alguna de la LOPD pues habría actuado en nombre y por cuenta de Ceac, es preciso recordar que el artículo 12 de la LOPD, al regular el "*Acceso a los datos por cuenta de terceros",* establece lo siguiente:
"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier

soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."
En el presente caso, Ceac en sus alegaciones afirma que no ha realizado una cesión de datos a la entidad Arvato, por cuanto la misma es simplemente un encargado del tratamiento de sus ficheros, en base al contrato de *"listbroking"* de fecha 2/12/2003, suscrito entre ambas entidades. En relación con dicho asunto, y además de lo señalado en el Fundamento de Derecho anterior, conviene recordar que en los Hechos Probados han quedado acreditados los siguientes extremos:
Ceac manifiesta que ha recabado el consentimiento de los interesados incluidos en el *"Fichero Maestro de Promociones".*
Ceac está interesada en que Arvato utilice su fichero en las promociones que le encarguen sus clientes, que actúan como beneficiarios de la publicidad.
Ceac facilita una copia completa del fichero a Arvato.
Arvato se compromete, antes de usar el fichero, a pedir autorización a Ceac y se constituye en representante de ésta para negociar los contratos de sus clientes.
Arvato realiza en su nombre los contratos con los beneficiarios de la publicidad y usa, a su juicio, tanto los ficheros propios como los de las entidades con las que ha suscrito un contrato de *"listbroking".*
Ceac factura a Arvato, según las consultas que ésta le confirma, deduciendo del precio su comisión.
Arvato factura, en su exclusivo nombre, al beneficiario de la publicidad según el contrato establecido al efecto.
Respecto a dicho asunto, en la Sentencia de la Audiencia Nacional, de 29/04/2005, la Sala aplica la siguiente doctrina:
"Se plantea en definitiva a la Sala el problema de la diferenciación entre la cesión y el encargado de tratamiento, "encargado de tratamiento" que no venía expresamente regulado en la LO 5/1992, pero entendía la doctrina que tenía cabida en lo establecido en el Art. 27. Siguiendo lo dispuesto en tal Directiva Europea 95/46/CE, la LO 15/1999 ha regulado específicamente la figura en los aludidos Art. 3.g) y 12, y de hecho la definición de "encargado de tratamiento" contenida en el Art. 3.g) no es sino trascripción del Art. 2.e) de la Directiva.
Y si bien la diferencia entre encargo de tratamiento y cesión, como reconoce la doctrina, en algunos casos es compleja, lo que es evidente es que no puede haber cesión cuando existe encargo de tratamiento y no resulta preciso el consentimiento del afectado.
Lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquél con el objeto dc prestarle un servicio en un ámbito concreto. Habría por tanto encargo de tratamiento en los supuestos de outsourcing o en los de prestación derivada de un contrato de obra o arrendamiento de servicios con un fin concreto. Siendo esencial, para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargo..."
"En definitiva xxx y xxxx accedieron a los datos personales del afectado, para prestar un servicio, más no a la cesionaria de tales datos, sino a las beneficiarias de la obtención de los mismos, por lo que de ningún modo su relación con xxx puede ser considerada como un encargado de tratamiento a tenor del art. 12 de la LOPD, y tal

pretensión ha de ser desestimada."(el subrayado es de la Agencia Española de Protección de Datos).
Asimismo otras sentencias de la Audiencia Nacional, también han tenido ocasión de referirse a esta cuestión:
En la Sentencia de 24/06/2003, la Sala ante un supuesto de pretendido contrato de arrendamiento de servicios por cuenta de tercero, que, a juicio del cesionario, le eximía de solicitar el consentimiento de los afectados, señaló que no se trataba de una auténtica prestación de servicios por cuenta de terceros porque para ello el tercero se debería de haber limitado a efectuar el tratamiento por cuenta del responsable, pero ello no fue así porque el tercero... *"no desaparece de la relación, sino que utiliza los datos en su provecho económico...",* cuando lo que debería ser es que el tercero recibiera su remuneración del responsable del fichero por cuenta del que trata sus datos.
En la Sentencia de 15/10/2004, reitera la doctrina anterior al señalar que no son incardinables en el artículo 12 de la LOPD, los supuestos en los que el tercero no actúa como encargado de tratamiento porque... *"no es encargado...en los términos previstos en el artículo 3.g) de la Ley 15/1999 (por cuanto no trata los datos personales por cuenta del responsable del tratamiento, sino en beneficio propio)..."*
De acuerdo con la doctrina señalada, no cabe deducir que del contrato suscrito entre Arvato y Ceac de 2/12/2003, aquélla se constituyera en encargado de tratamiento de ésta ya que ha quedado acreditado que Arvato actuó, en todo momento, ejecutando un contrato suscrito con el beneficiario de la publicidad, es decir, en beneficio propio, facturando a éste y confirmando a Ceac los datos obtenidos de sus ficheros para descontar su comisión por la actividad desarrollada por su cuenta.

VIII

El artículo 6. 1 y 2 de la LOPD disponen lo siguiente:
"*1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencia; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado."
De acuerdo con lo señalado en el Fundamento de Derecho anterior, Arvato, al no actuar como encargado de tratamiento de Ceac, necesitaba del consentimiento del denunciante para poder tratar sus datos en su propio beneficio, sin que haya quedado acreditada dicha circunstancia y sin que concurriera ninguna de las causas establecidas en el apartado 2 de dicho artículo para que no fuese preciso su consentimiento.

IX

La hoy derogada Ley Orgánica 5/1992, de 29/10, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (en lo sucesivo LORTAD), delimitaba su ámbito de aplicación en torno al concepto de fichero automatizado (art. 2), que figuraba definido como "*todo conjunto organizado de datos de carácter personal que*

sean objeto de tratamiento automatizado (...)". Congruentemente con dicha configuración legal, la LORTAD se limitaba a definir la figura del responsable del fichero (art. 3.b) y d)).
Por el contrario, la vigente LOPD ha modificado el ámbito de aplicación objetivo de la norma circunscribiéndola a "*los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento automatizado, y a toda modalidad de uso posterior a estos datos (...)*" (art. 2). De acuerdo con esta delimitación, la LOPD modifica la definición del fichero y diferencia las figuras del responsable del fichero y del responsable del tratamiento (art. 3.b. y d.). Asimismo delimita con precisión la figura del encargado del tratamiento (art. 12). El artículo 3 de la LOPD establece lo siguiente:
"b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso."
"d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento."
Esta modificación es congruente con las exigencias de la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos, que la LOPD incorpora a nuestro derecho, conforme a la cual, en el caso de los datos personales susceptibles de tratamiento automatizado, la Ley se aplica no sólo cuando existe un conjunto organizado (fichero) de dichos datos, sino también cuando se realizan operaciones y procedimientos que permitan la recogida, grabación, conservación, elaboración, bloqueo y cancelación de aquellos, aunque el responsable de ese tratamiento carezca de bases de datos de su titularidad que, de acuerdo con los términos legales, se incluyen en la definición de fichero.
Conforme se ha señalado, cabe que el sistema de protección de la LOPD se exija a los responsables del tratamiento, aunque carezcan de ficheros, e incluso, a los meros encargados de aquél, a los que la LOPD también puede convertir en responsables (art. 12.4).
Por lo demás, la configuración legal se adecúa perfectamente a la realidad en la que cada vez es más frecuente la externalización de los servicios informáticos, que no son prestados por las propias empresas responsables de los ficheros sino por terceros. Así, cabe citar como caso paradigmático, la gestión de recursos humanos de las empresas que, en números ocasiones, no determinan la creación de ficheros automatizados por parte del empresario, sino que se encomiendan a empresas o profesionales especializados sin que esta ausencia de ficheros determine que no sea aplicable la LOPD, pues el empresario es responsable del tratamiento ya que es quien decide sobre la finalidad, contenido y uso del tratamiento.
Una interpretación contraria llevaría a que el sistema de protección de datos pudiera quedar vacío de tutela respecto de un número cada vez mayor de tratamientos que se externalizan.
Dentro del marco expuesto, en el presente caso ha quedado acreditado que el tratamiento de los datos del denunciante, para la remisión del escrito publicitario lo realizó Arvato.
Arcadia alega que fue la beneficiaria de la campaña de "*marketing*" remitida al denunciante, y que la entidad Arvato no le entregó los listados para la remisión de las cartas publicitaria, ni le comunicó el nombre de los destinatarios.
Por todo, con independencia de que el tratamiento de los datos del denunciante se haya realizado directamente por Arvato, sin embargo, de la documentación obrante en el presente procedimiento, resulta evidente que quien decidió, en definitiva, sobre la finalidad, contenido y uso de la campaña publicitaria fue Arcadia.

En efecto, la empresa citada ha decidido que se realice una campaña publicitaria, ha delimitado el colectivo de personas físicas identificadas o identificables a las que debía realizarse el envío publicitario al contratar la selección de los destinatarios, y ha determinado la finalidad y uso del tratamiento de los datos de las personas seleccionadas al contratar el envío de una comunicación publicitaria de sus productos, de la que, lógicamente la propia entidad es la beneficiaria.
El citado artículo 3.d) de la LOPD, arriba transcrito, considera como responsable del tratamiento no sólo al titular o responsable del fichero, sino también a la persona física o jurídica *"que decida sobre la finalidad, contenido y uso del tratamiento"*, de donde resulta que Arcadia, al haber decidido sobre la finalidad, contenido y uso de la campaña publicitaria de referencia es responsable del tratamiento de los datos personales en ella utilizados, por lo que ha cometido la infracción descrita en el citado art. 44.3.d) de la LOPD, por cuanto el tratamiento realizado de los datos personales del denunciante se efectuó sin contar con su consentimiento y sin que concurriera ninguna de las causas de exclusión del consentimiento contempladas en el artículo 6 de la LOPD.
En el presente caso, ha quedado acreditado un tratamiento de datos sin consentimiento del denunciante, por parte de ambas entidades, lo que supone sendas infracciones del artículo 6.1, tipificadas como graves en el artículo 44.3.d) de la LOPD.

X

El artículo 44.3.d) de la LOPD considera infracción grave: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley, o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*.
La Audiencia Nacional ha manifestado, en su Sentencia de 22/10/03, que *"la descripción de conductas que establece el artículo 44.3d) de la Ley Orgánica 15/1999 cumple las exigencias derivadas del principio de tipicidad, a juicio de esta Sala, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. En efecto, el tipo aplicable considera infracción grave "tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la Ley", por tanto, se está describiendo una conducta –el tratamiento automatizado de datos personales o su uso posterior- que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la Ley Orgánica. Ahora bien, estos principios no son de aquellos que deben inferirse de dicha regulación legal, sino que aparecen claramente determinados y relacionados en el título II de la Ley, concretamente, por lo que ahora interesa, en el artículo 6 se recoge un principio que resulta elemental en la materia, que es la necesidad de consentimiento del afectado para que puedan tratarse automatizadamente datos de carácter personal. Por tanto, la conducta ilícita por la que se sanciona a la parte recurrente como responsable del tratamiento consiste en usar datos sin consentimiento de los titulares de los mismos, realizando envíos publicitarios."*
De acuerdo con lo señalado con anterioridad, tanto Arcadia como Arvato vulneraron el principio del consentimiento, recogido en el artículo 6 de la LOPD, lo que encuentra su tipificación en el citado artículo 44.3.d) de la citada Ley Orgánica.

XI

No pueden ser tenidas en cuenta las alegaciones de Ceac, en el sentido de que su cláusula informativa había sido informada favorablemente por esta Agencia Española de Protección de Datos, por cuanto que, como ya se ha señalado, la cláusula utilizada

para la recogida de datos del denunciante, se recogía *"... que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollen su actividad en los sectores..."*, y no se corresponde con la informada por la Agencia por cuanto en la primera se establecía que "...*a que comunique tales datos a otras empresas del Grupo Planeta cuyas actividades se relacionen..."*

XII

Por otro lado, el artículo 49 de la LOPD señala: "*En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido la Agencia Española de Protección de Datos podrá., mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas."*

XIII

El artículo 45.2, 3 y 4 de la LOPD establece:
"2. Las infracciones graves serán sancionadas con multas de 60.101,21 € a 300.506,05 €.
3. Las infracciones muy graves serán sancionadas con multas de 300.506,05 € a 601.012,01 €
4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora."
La aplicación con carácter excepcional del citado artículo 45.5 exige la concurrencia de, al menos, uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuricidad del hecho.
Durante la tramitación del presente procedimiento, ha quedado acreditado que Arcadia actuó en la creencia de que al no tratar en ningún momento datos de carácter personal, en ningún caso su conducta podría vulnerar, como así ha sido, el artículo 6 de la LOPD. En relación a este asunto, como mayor garantía, contrató con Arvato la promoción de la campaña publicitaria que ha dado lugar al presente procedimiento sancionador. En consecuencia se considera que concurre una disminución cualificada de la culpabilidad que permite aplicar a Arcadia el artículo 45.5 de la LOPD.
En el caso de Ceac, ha quedado acreditado, como asimismo dicha entidad reconoce, que se apartó de la cláusula informativa que había sido sometida a informe del Gabinete Jurídico de esta Agencia, deduciéndose de la finalmente implementada diferencias sustanciales que permiten deducir que los interesados no prestaron su consentimiento inequívoco para la comunicación de sus datos con fines publicitarios. Por dicho motivo, no se observan motivos que permitan aplicar, en el presente supuesto, el artículo 45.5 a la citada entidad.

Asimismo, en relación a los criterios de graduación de las sanciones recogidos en el artículo 45.4 de la LOPD, y en especial, en función de la ausencia de intencionalidad y de reincidencia acreditadas a lo largo del presente procedimiento, procede imponer a la entidad Arvato una sanción de 60.101,21 €, a la entidad Arcadia una sanción de 6.000 €, y a la entidad Ceac una sanción de 300.506,05 €.
Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: IMPONER a la entidad **ARCADIA INTERNACIONAL, S.A.,** por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 6.000 € (seis mil euros) de conformidad con lo establecido en el artículo 45.2, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: IMPONER a la entidad **ARVATO SERVICES IBERIA S.A.,** por una infracción del artículo 6.1 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 60.101,21 € (sesenta mil ciento un euros con veintiun céntimos de euro) de conformidad con lo establecido en el artículo 45.2 y 4 de la citada Ley Orgánica.

TERCERO: IMPONER a la entidad **CENTRO DE ESTUDIOS CEAC S.L.**, por una infracción del artículo 11 de la LOPD, tipificada como muy grave en el artículo 44.4.b) de dicha norma, una multa de 300.506,05 € (trescientos mil quinientos seis euros con cinco céntimos de euro) de conformidad con lo establecido en el artículo 45.3 y 4 de la citada Ley Orgánica.

CUARTO: REQUERIR a **CENTRO DE ESTUDIOS CEAC S.L.**, para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 11 de la LOPD, con indicación de que, de acuerdo con lo preceptuado en le artículo 49 de la citada Ley Orgánica, si el requerimiento fuera desatendido la Agencia Española de Protección de Datos podrá inmovilizar el fichero.
Las medidas y actuaciones adoptadas deberán ser comunicadas a esta Agencia Española de Protección de Datos, en el plazo de un mes.
QUINTO: NOTIFICAR la presente resolución a **ARCADIA INTERNACIONAL, S.A.**, (C/.....), a **ARVATO SERVICES IBERIA S.A.**, (C/.....), a **CENTRO DE ESTUDIOS CEAC S.L.**, (C/.....), y a **D. J.B.S.**, (C/.....).

SEXTO: Advertir a los sancionados que las sanciones impuestas deberán hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si reciben la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si reciben la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.
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.
Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Procedimiento Nº PS/00476/2009

RESOLUCIÓN: R/02619/2009

En el procedimiento sancionador PS/00476/2009, instruido de oficio por la Agencia Española de Protección de Datos a **DON M.M.M. (COLEGIO YOCRIS)**, vista la denuncia presentada ante la misma,

ANTECEDENTES

PRIMERO: Con fecha 12 de diciembre de 2008, el Director de la Agencia Española de Protección de Datos solicitó la apertura de actuaciones de inspección ante el Colegio Yocris de (.....), a la vista de un escrito presentado en esta Agencia por una agrupación de padres en el que ponen de manifiesto que en el citado Colegio se han instalado cámaras de videovigilancia que graban imágenes del interior del centro escolar y de la vía pública.

SEGUNDO: A la vista de los citados hechos, el Director de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos la realización de las actuaciones previas de investigación para el esclarecimiento de los hechos, teniendo conocimiento de los siguientes extremos:
Con fecha 20 de mayo de 2009, se giró visita de Inspección en la sede del Colegio Yocris, habiéndose constatado lo siguiente:
1 Don M.M.M. realizó las siguientes manifestaciones en respuesta a las preguntas formuladas por los inspectores de la Agencia:
1.1 Don M.M.M. es propietario del colegio YOCRIS de carácter privado que imparte enseñanza oficial de educación infantil, primaria y secundaria. Así mismo, reside en el mismo colegio conde tiene su vivienda.
1.2 El sistema de video vigilancia ha sido instalado en el colegio hace aproximadamente un año por la empresa DISISAT COMUNICACIONES, S.L. inscrita en el Registro de Instalaciones de Comunicación con el número ***. Don M.M.M. aportó copia de la factura emitida con fecha 2 de febrero de 2009 emitida por la citada empresa para el cobro de parte de los servicios y suministros realizados.
1.3 En el centro escolar tiene instaladas un total de once cámaras de vídeo distribuidas en las siguientes ubicaciones:
_ Una se encuentra instalada en la parte exterior del centro tomando imágenes de la puerta exterior y la porción de acera de entrada al centro, donde aparcan los alumnos las bicicletas.
_ Dos instaladas en el patio del centro, una tomando imágenes del patio y la otra de la puerta de entrada.
_ Una en el gimnasio
_ Una en la cocina
_ Una en cada una de las cuatro clases de enseñanza secundaria.
_ Una en el pasillo de acceso a las clases del primer piso y otra en el del segundo piso.
1.4 Las imágenes son visualizadas exclusivamente por Don M.M.M..
1.5 Para la visualización de las imágenes dispone de cuatro monitores y una pantalla digital ubicados en despacho del Director y vivienda particular del mismo.
1.6 Las imágenes son reproducidas en tiempo real y no son grabadas en ningún soporte.
1.7 Dispone de carteles informativos según modelo dispuesto en la Instrucción1/2006, de la Agencia Española de Protección de Datos colocados en todas las puertas de acceso al centro.

1.8 La finalidad para la que ha sido instalado el sistema de video vigilancia es por motivos de seguridad.
2 Los inspectores de la Agencia solicitaron a Don M.M.M. que les mostrara el sistema en el que se reproducen las imágenes, trasladándose al despacho del Director del Centro, donde se realizan las siguientes comprobaciones:
2.1 Se comprueba la existencia de cuatro monitores que en el momento de la inspección se encuentran reproduciendo imágenes en tiempo real de un pasillo, de una de las clases de secundaria, del patio y de la puerta de entrada.
2.2 Se comprueba la existencia de una pantalla digital que reproduce en distintas ventanas las imágenes en tiempo real correspondientes a tres clases de secundaria, uno de los pasillos, el gimnasio, la cocina y la cámara exterior. Se comprueba que la cámara recoge imágenes de la porción de acera de entrada al centro, comprobando que se encuentra aparcadas algunas bicicletas.
2.3 Se comprueba que los monitores no están conectados a ningún ordenador.
3 Los inspectores de la Agencia comprobaron la existencia de las cámaras de video relacionadas en el punto 3.3 de esta Acta.
4 Los inspectores de la Agencia comprobaron que existen un total de cinco carteles informativos colocados en las puertas de acceso exterior e interiores al centro.
5 Los padres, alumnos y profesores del centro escolar han sido informados verbalmente de la existencia del sistema de video vigilancia.

TERCERO: A la vista del resultado de estas actuaciones previas de investigación, con fecha 8 de junio de 2006, el Director de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **DON M.M.M.,** con arreglo a lo dispuesto en el artículo 127 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, por la presunta infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3. d) de la citada Ley Orgánica pudiendo ser sancionado con multa de 60.101,21 € a 300.506,05 €, de acuerdo con el artículo 45.2 de la LOPD.

CUARTO: Notificado el acuerdo de inicio a Don M.M.M., en fecha 2 de octubre de 2009, de acuerdo con la comunicación de recibo emitido por el Servicio de Correos, el denunciado no ha presentado alegaciones al respecto.

QUINTO: El artículo 13.2 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, señala que:
"El acuerdo de iniciación se comunicará al instructor, con traslado de cuantas actuaciones existan al respecto, y se notificará al denunciante, en su caso, y a los interesados, entendiendo en todo caso por tal al inculpado. En la notificación se advertirá a los interesados que, de no efectuar alegaciones sobre el contenido de la iniciación del procedimiento en el plazo previsto en el artículo 16.1, la iniciación podrá ser considerada propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, con los efectos previstos en los artículos 18 y 19 del Reglamento."
Dado que la notificación del acuerdo de inicio del procedimiento sancionador a Don M.M.M. se ha realizado de forma fehaciente, y que el denunciado no ha realizado alegaciones, se considera el mencionado acuerdo de inicio como propuesta de resolución

HECHOS PROBADOS

PRIMERO: Con fecha 12 de diciembre de 2008, el Director de la Agencia Española de Protección de Datos solicitó la apertura de actuaciones de inspección ante el Colegio Yocris de (.....), a la vista de un escrito presentado en esta Agencia por una agrupación de padres en el que ponen de manifiesto que en el citado Colegio se han instalado cámaras de videovigilancia que graban imágenes del interior del centro escolar y de la vía pública (folios 1-6).

SEGUNDO: Con fecha 20 de mayo de 2009, se giró visita de Inspección durante la cual Don M.M.M. realizó las siguientes manifestaciones en respuesta a las preguntas formuladas por los inspectores de la Agencia:
- Don M.M.M. es propietario del colegio YOCRIS de carácter privado que imparte enseñanza oficial de educación infantil, primaria y secundaria. Asimismo, reside en el mismo colegio donde tiene su vivienda.
- El sistema de video vigilancia ha sido instalado en el colegio hace aproximadamente un año por la empresa DISISAT COMUNICACIONES, S.L. inscrita en el Registro de Instalaciones de Comunicación con el número 4880. Don M.M.M. aportó copia de la factura emitida con fecha 2 de febrero de 2009 emitida por la citada empresa para el cobro de parte de los servicios y suministros realizados.
- En el centro escolar tiene instaladas un total de once cámaras de vídeo distribuidas en las siguientes ubicaciones:
_ Una se encuentra instalada en la parte exterior del centro tomando imágenes de la puerta exterior y la porción de acera de entrada al centro, donde aparcan los alumnos las bicicletas.
_ Dos instaladas en el patio del centro, una tomando imágenes del patio y la otra de la puerta de entrada.
_ Una en el gimnasio
_ Una en la cocina
_ Una en cada una de las cuatro clases de enseñanza secundaria.
_ Una en el pasillo de acceso a las clases del primer piso y otra en el del segundo piso.
- Las imágenes son visualizadas exclusivamente por Don M.M.M..
- Para la visualización de las imágenes dispone de cuatro monitores y una pantalla digital ubicados en despacho del Director y vivienda particular del mismo.
- Las imágenes son reproducidas en tiempo real y no son grabadas en ningún soporte.
- Dispone de carteles informativos según modelo dispuesto en la Instrucción1/2006, de la Agencia Española de Protección de Datos colocados en todas las puertas de acceso al centro.
- Los padres, alumnos y profesores del centro escolar han sido informados verbalmente de la existencia del sistema de video vigilancia.
- La finalidad para la que ha sido instalado el sistema de video vigilancia es por motivos de seguridad (folios 9-10)

TERCERO: Los inspectores de la Agencia solicitaron a Don M.M.M. que les mostrara el sistema en el que se reproducen las imágenes, trasladándose al despacho del Director del Centro, donde se realizan las siguientes comprobaciones:
- Se comprueba la existencia de cuatro monitores que en el momento de la inspección se encuentran reproduciendo imágenes en tiempo real de un pasillo, de una de las clases de secundaria, del patio y de la puerta de entrada.
- Se comprueba la existencia de una pantalla digital que reproduce en distintas ventanas las imágenes en tiempo real correspondientes a tres clases de secundaria, uno de los pasillos, el gimnasio, la cocina y la cámara exterior. Se comprueba que la cámara recoge imágenes de la porción de acera de entrada al centro, comprobando que se encuentra aparcadas algunas bicicletas.
- Se comprueba que los monitores no están conectados a ningún ordenador.

- Los inspectores de la Agencia comprobaron la existencia de las cámaras de video relacionadas en el punto 3.3 del Acta de Inspección.
- Los inspectores de la Agencia comprobaron que existen un total de cinco carteles informativos colocados en las puertas de acceso exterior e interiores al centro (folios 10-11).

CUARTO: No consta acreditado que la instalación o mantenimiento de las cámaras la haya realizado una empresa de seguridad autorizada, ya que de la factura aportada por el denunciado, relativa a la empresa DISISAT COMUNICACIONES, S.L, no se desprende información que permita justificar la instalación del sistema de videovigilancia. Tampoco consta autorización administrativa al respecto (folio 13).

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

Con carácter previo, debe señalarse que el artículo 1 de la LOPD dispone: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*
La LOPD, viene a regular el derecho fundamental a la protección de datos de las personas físicas, esto es, el derecho a disponer de sus propios datos sin que puedan ser utilizados, tratados o cedidos sin su consentimiento, con la salvedad de las excepciones legalmente previstas.
En cuanto al ámbito de aplicación de la citada norma, el artículo 2.1 de la misma señala: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado";* definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *"Cualquier información concerniente a personas físicas identificadas o identificables".*
El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones*, *consultas, interconexiones y transferencias*". La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.
El artículo 5.1. f) 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, define datos de carácter personal como: *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, 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 personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *"toda información sobre una persona física identificada o identificable; 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"*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.
De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

III

La Directiva 95/46/CE en su Considerando 14 afirma:
"(14)Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;". 7/16 El Grupo de protección de las personas, en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la citada Directiva 95/46/CE, en su Dictamen 4/2004, adoptado en fecha 11/02/2004, relativo al tratamiento de datos personales mediante vigilancia por videocámara, formula distintos criterios para evaluar la legalidad y conveniencia de instalar sistemas de captación de imágenes en zonas públicas.
Por otra parte, para determinar si el supuesto que se analiza implican el tratamiento de datos relacionados con personas identificables, el citado Grupo considera que los datos constituidos por imagen y sonido son personales aunque las imágenes se utilicen en el marco de un sistema de circuito cerrado y no estén asociados a los datos personales del interesado, incluso, si no se refieren a personas cuyos rostros hayan sido filmados, e independientemente del método utilizado para el tratamiento, la técnica, el tipo de equipo, las características de la captación de imágenes y las herramientas de comunicación utilizadas. A efectos de la Directiva, se añade, el carácter identificable también puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos.
En cuanto a las obligaciones y precauciones que deberán respetarse por los responsables del tratamiento de los datos se mencionan, entre otras, la de evitar las referencias inadecuadas a la intimidad; especificar de forma clara e inequívoca los fines perseguidos con el tratamiento y otras características de la política de privacidad (momento en que se borran las imágenes, peticiones de acceso); obtención del consentimiento del interesado basado en una información clara; mantener la necesaria proporcionalidad entre los datos y el fin perseguido, obligándose al empleo de sistemas idóneos con respecto a dicho fin y a minimizar los datos por parte del responsable del tratamiento; datos que han de ser adecuados, pertinentes y no excesivos y deberán retenerse durante un plazo en consonancia con las características específicas de cada caso.

Por tanto, la captación de imágenes con fines de vigilancia y control, como es el caso que nos ocupa, se encuentra plenamente sometida a lo dispuesto en la LOPD, ya que constituye un tratamiento de datos de carácter personal.
De acuerdo con los preceptos transcritos, la videocámara reproduce la imagen de los afectados por este tipo de tratamientos y, a efectos de la LOPD, la imagen de una persona constituye un dato de carácter personal, toda vez que la información que capta concierne a personas y suministra información sobre la imagen personal de éstas, el lugar de su captación y la actividad desarrollada por el individuo al que la imagen se refiere. En el caso que nos ocupa, en el Acta emitida por la Inspección de Datos, en fecha 20 de mayo de 2009, se constató, mediante la inspección realizada en el Colegio Yocris en (.....), a nombre de DON M.M.M., S.A., hay instaladas once cámaras de videovigilancia instaladas en los siguientes puntos: *"Una se encuentra instalada en la parte exterior del centro tomando imágenes de la puerta exterior y la porción de acera de entrada al centro, donde aparcan los alumnos las bicicletas. Dos instaladas en el patio del centro, una tomando imágenes del patio y la otra de la puerta de entrada. Una en el gimnasio. Una en la cocina. Una en cada una de las cuatro clases de enseñanza secundaria. Una en el* 8/16 *pasillo de acceso a las clases del primer piso y otra en el del segundo piso"* , sin tener autorización para ello.

IV

Para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: *"La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública".*
Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: *"Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*
e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia".
En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, y además en el mismo texto legal se regulan los criterios para instalar las cámaras y los derechos de los interesados.
En el presente caso, las cámaras ubicadas en las fachadas exteriores del Colegio Yocris captaban imágenes de los viandantes sin que tuvieran autorización administrativa al respecto, puesto que como ya se ha establecido *"ut supra*", la instalación de cámaras en la vía pública es competencia exclusiva de los Fuerzas y Cuerpos de Seguridad del Estado.

V

En cuanto al carácter proporcional, idóneo y necesario de la medida de instalación de cámaras de videovigilancia hay que señalar que el artículo 4.1 y 2 de la LOPD,

garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala que:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".

En este sentido, el citado Dictamen 4/2004, del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre 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, relativo al tratamiento de datos personales mediante vigilancia por videocámara, apartado D), señala lo siguiente:

"D) Proporcionalidad del recurso a la vigilancia por videocámara.

El principio según el cual los datos deberán ser adecuados y proporcionales al fin perseguido significa, en primer lugar, que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas. Dicho principio de proporcionalidad supone que se pueden utilizar estos sistemas cuando otras medidas de prevención, protección y seguridad, de naturaleza física o lógica, que no requieran captación de imágenes (por ejemplo, la utilización de puertas blindadas para combatir el vandalismo, la instalación de puertas automáticas y dispositivos de seguridad, sistemas combinados de alarma, sistemas mejores y más potentes de alumbrado nocturno en las calles, etc.) resulten claramente insuficientes o inaplicables en relación con los fines legítimos mencionados anteriormente".

En este sentido, se pronuncia la Instrucción 1/2006, cuando señala en el artículo 4, lo siguiente:

"1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida".

La aplicación de estos principios resulta especialmente relevante, dado que la instalación de dicho sistema de seguridad debe ser como consecuencia de que se hayan producido en repetidas y números ocasiones determinadas conductas violentas.

Así para el efectivo cumplimiento de los principios indicados, en especial los relativos a la proporcionalidad, finalidad de los medios utilizados para el servicio de videovigilancia, se debe señalar que en aquellos casos en los que los dispositivos instalados tengan la capacidad de captar o registrar tanto imágenes como sonidos mediante técnicas desproporcionadas para la finalidad del tratamiento, como podrían ser dispositivos móviles, direccionables, de ampliación de imágenes o posibilidad de

enfoque de imágenes ajenas a la finalidad concreta y específica de videovigilancia, sin que de ningún modo la videovigilancia afecte a la vía pública, puesto que en ese caso la competencia es exclusiva de los Cuerpos y Fuerzas de Seguridad del Estado de conformidad con lo dispuesto en la Ley Orgánica 4/1997, el responsable de tales tratamientos deberá responder de la responsabilidad que en su caso incurra.
Asimismo, en el preámbulo de la citada Instrucción 1/2006, señala lo siguiente:
"En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.
En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo funciones de vigilancia por lo que, desde un punto de vista objetivo, la utilización de estos sistemas debe ser proporcional al fin perseguido, que en todo caso deberá ser legítimo.
En cuanto a la proporcionalidad, pese a ser un concepto jurídico indeterminado, la Sentencia del Tribunal Constitucional 207/1996 determina que se trata de «una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.
En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones <<si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)".
El principio de moderación en el uso de datos personales, debería aplicarse en todos los sectores, teniendo en cuenta, también el hecho de que muchos objetivos pueden alcanzarse realmente sin recurrir a datos personales.
En consecuencia cualquier medida que permita preservar la seguridad, sin necesidad de implementar sistemas de videovigilancia, deberá de aplicarse con preferencia. Asimismo de existir con anterioridad medidas que garanticen la seguridad sin necesidad de acudir a sistemas de videovigilancia y aquellas resulten eficaces, deberá prevalecer el mantenimiento de dichas medidas, en aras de proteger la intimidad de las personas.
Respecto a la posibilidad de captar un pequeño ángulo de la vía pública a través de una cámara instalada por una empresa de seguridad privada, ésta deberá cumplir con el principio de proporcionalidad, sin que sea posible extender la grabación de imágenes a un alcance mayor al que resulte necesario para garantizar la seguridad de las instalaciones.
Por ello, la referencia a los *"alrededores"* de las instalaciones, únicamente resultaría ajustada a la normativa de protección de datos en caso de que la misma se refiera exclusivamente a aquellos espacios sin cuya grabación resultaría en todo punto imposible el control de la seguridad en el acceso a las instalaciones, sin que en modo alguno esta referencia pueda entenderse efectuada, con carácter general a la vía pública.
En el caso que nos ocupa, en ningún caso puede considerarse la instalación de dicho sistema de videovigilancia proporcional, desde el momento que se acredita por el

Informe de la Inspección que la visualización que se produce de la vía pública es excesiva en relación con la finalidad que ha justificado su instalación, por cuanto capta imágenes de la vía pública. Por otra parte, se estima que no resulta proporcional la instalación de cámaras de videovigilancia en las aulas.

VI

Se imputa al denunciado la comisión de una infracción del artículo 6 de la LOPD, que dispone lo siguiente:
"*1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.*
2. *No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado*.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".
El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), "...*consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.
En el caso analizado, las imágenes captadas por las cámaras son datos de carácter personal conforme al artículo 3.a) de la LOPD y al artículo 5.1. f) del citado Real Decreto 1720/2007, toda vez que las cámaras captan imágenes de las personas que circulan por la vía pública. Asimismo, tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.
Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.
En el presente procedimiento, el denunciado capta datos personales. Dichas imágenes, capturadas constituyen datos personales, y por tanto sometidos al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD.
El artículo 3 de la LOPD define en su apartado h), lo siguiente:

"h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".
Por lo tanto, el consentimiento del interesado para el tratamiento de sus datos debe ser *"informado", "específico", "inequívoco" y "libre",* o bien, que no sea necesario tal consentimiento al contar el sistema de vídeovigilancia de habilitación legal conforme dispone el segundo inciso del citado artículo 6.1 de la LOPD.
En relación con el segundo inciso del artículo 6.1 de la LOPD, tampoco ha quedado acreditado que el sistema de vídeovigilancia de la entidad denunciada estuviera acogido a las disposiciones de la Ley Orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, por lo que el tratamiento de los datos recogidos en la vía pública carecía de habilitación legal. 13/16

VII

El artículo 44.3.d) de la LOPD tipifica como infracción grave: *"Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave".*
En relación al tipo de infracción establecido en el citado artículo 44.3.d), la Audiencia Nacional, en Sentencia de 27/10/2004, ha declarado: *"Sucede así que, como ya dijimos en la Sentencia de 8 de octubre de 2003 (recurso 1.821/01) el mencionado artículo 44.3 d) de la Ley Orgánica 15/1999, aún no siendo, ciertamente, un modelo a seguir en lo que se refiere a claridad y precisión a la hora de tipificar una conducta infractora, no alberga una formulación genérica y carente de contenido como afirma la demandante. La definición de la conducta típica mediante la expresión "tratar los datos de carácter personal .." no puede ser tachada de falta de contenido pues nos remite directamente a cualquiera de las concretas actividades que el artículo 3.d) de la propia Ley incluye en la definición de "tratamiento de datos" (recogida, grabación, conservación, elaboración, ... de datos de carácter personal). Y tampoco cabe tachar de excesivamente genérico o impreciso el inciso relativo a que el tratamiento o uso de los datos se realice "... con conculcación de los principios y garantías establecidos en la presente Ley...", pues tales principios y garantías debidamente acotados en el Título II del propio texto legal bajo las rúbricas de Principios de la Protección de Datos (artículos 4 a 12) y Derechos de las Personas (artículos 13 a 19)".*
En el presente caso, la descripción de conductas que establece el artículo 44.3.d) de la LOPD cumple las exigencias derivadas del principio de tipicidad, toda vez que del expresado precepto se desprende con claridad cuál es la conducta prohibida. El tipo aplicable considera infracción grave *"tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley"*, por tanto, se está describiendo una conducta - el tratamiento automatizado de datos personales o su uso posterior – que precisa, para configurar el tipo, que dicha conducta haya vulnerado los principios que establece la LOPD.
En este caso, el denunciado han incurrido en la infracción grave descrita ya que el consentimiento para el tratamiento de los datos personales es un principio básico del derecho fundamental a la protección de datos, recogido en el artículo 6 de la LOPD , habiendo tratado datos de las personas que pudieran haber sido captadas por las cámaras de videovigilancia sin contar con su consentimiento, lo que supone una vulneración de este principio, conducta que encuentra su tipificación en este artículo 44.3.d).

VIII

El artículo 45.2, 4 y 5 de la LOPD establece lo siguiente: 14/16
"2. Las infracciones graves podrán ser sancionadas con multas de 60.101,21 € a 300.506,05 €".
"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora."
"5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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."
La aplicación con carácter excepcional del artículo 45.5 exige la concurrencia de al menos uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuricidad del hecho.
En relación con la aplicación del artículo 45.5 de la LOPD, la Audiencia Nacional ha señalado, entre otras, en Sentencia de 27/10/2004, que "*el citado precepto concreta el principio de proporcionalidad (reconocido para el Derecho administrativo sancionador, con carácter general, en el art. 131.3 de la Ley 30/1992), permitiéndose la disminución en un grado de la sanción aplicable en casos de cualificada disminución de la culpa o de la antijuridicidad. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor de justicia (art. 1.1 CE), por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos. Pues bien, en el caso de autos, la Sala entiende que dicho precepto no es de aplicación porque a la antijuridicidad no obsta la falta de intención de infringir las normas jurídicas (Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 4 de junio de 1999), y ya hemos razonado la falta de diligencia de la entidad recurrente".*
En conclusión, en el presente caso ha quedado acreditado que el denunciado tenían instaladas once cámaras de videovigilancia, sin que obre contrato de instalación por parte de empresa de seguridad autorizada. Además, ha quedado acreditado que de entre las once cámaras instaladas, algunas de ellas se encontraban en la fachada del colegio, que recogían y captaban imágenes de la vía pública, y otras se encontraban ubicadas en el interior de las aulas, superando el principio de proporcionalidad, establecido en materia de protección de datos, por lo que procede la imposición de sanción. Sin embargo, debido a que del Acta de la Inspección se desprende que el denunciado instaló el sistema en la creencia de que era legal y dado que no consta acreditado que en la actualidad las cámaras continúen captando imágenes procede imponer la sanción en la cuantía de 2.500 euros. No obstante, de no haberlo hecho, deberá proceder a retirar las citadas cámaras, o proceder a la adecuación de la legalidad vigente. 15/16
Vistos los preceptos citados y demás de general aplicación,
El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: IMPONER a **DON M.M.M.,** por una infracción del artículo 6 de la LOPD, tipificada como grave en el artículo 44.3.d) de dicha norma, una multa de 2500 € (dos

mil quinientos euros) de conformidad con lo establecido en el artículo 45.1, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: REQUERIR a **DON M.M.M., S.A.**, para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 6 de la LOPD, y, en concreto, que retire las cámaras de videovigilancia o, en su defecto, las adecue a la legalidad vigente.

TERCERO: NOTIFICAR la presente resolución a **DON M.M.M. (COLEGIO YOCRIS).**

CUARTO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso en la cuenta restringida nº 0000 0000 00 0000000000 abierta a nombre de la Agencia Española de Protección de Datos en el Banco Bilbao Vizcaya Argentaria, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo. Si recibe la notificación entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si recibe la notificación entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.
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, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora 16/16
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.

Procedimiento nº: PS/00219/2009

ASUNTO: Recurso de Reposición Nº RR/00575/2009

Examinado el recurso de reposición interpuesto por la entidad Centro Organizado de Enseñanza a Distancia S.L. contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00219/2009, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 7 de septiembre de 2009, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00219/2009 , en virtud de la cual se imponía a la entidad denunciado, una sanción de 60.101,21 €, por la vulneración de lo dispuesto en el artículo 16 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como grave en el artículo 44.3 f) , de conformidad con lo establecido en el artículo 45 de la citada Ley Orgánica.

Dicha resolución, que fue notificada al recurrente en fecha 9 de septiembre de 2009, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en el artículo 127 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00219/2009, quedó constancia de los siguientes:

HECHOS PROBADOS

PRIMERO.- Mediante escrito de fecha de 16 de junio de 2007 (Folio 3) el denunciante se dirigió a EUROCEP para ejercer su derecho de cancelación.

SEGUNDO.- Mediante escrito de fecha de 11 de julio de 2007, EUROCEP, comunica al denunciante lo siguiente: "Por el presente, y atendiendo a su atento escrito, le comunicamos que sus datos personales han sido suprimidos de nuestro fichero. El origen de los datos utilizados proviene de nuestra propia base de datos formada en virtud de contestaciones a constantes campañas publicitarias efectuadas por nuestra entidad mediante impresos postales sin dirección contratado por el Organismo de Correos, Prensa, Internet y otros." . Figurando en dicho escrito los siguientes datos R.R.R., (C/.....).

TERCERO.- Mediante comunicación comercial de junio de 2008, EUROCEP vuelve a tratar los datos personales del denunciante, constando en dicho escrito los siguientes: R.R.R., (C/.....). (Folios 5 Y 6) Evidenciando por tanto una modificación en los mismos, con posterioridad a la comunicación de fecha de 11 de julio de 2007.

CUARTO.- EUROCEP no ha acreditado el origen de los datos personales del denunciante y el consentimiento de éste, ni con anterioridad al escrito de 11 de julio de 2007, ni para el tratamiento relativo a la comunicación comercial de 2008 (Folio 5 Y 6) con posterioridad a la confirmación de la cancelación de sus datos, evidenciando que dicha cancelación no se llevó a cabo.

QUINTO.- A requerimiento de esta Agencia, en fecha de 23 de octubre de 2008, EUROCEP manifestó que "hemos podido comprobar que el denunciante remitió el pasado año una solicitud de cancelación que esta parte atendió en tiempo y forma, procediendo a bloquear sus datos incluyéndolos en al Lista Robinson.

El hecho de que haya recibido el denunciante un nuevo envío el presente año, debe ser a un error involuntario del programa informático, por cuanto hemos vuelto a comprobar ahora que sus datos se encuentran debidamente bloqueados" (folio 25)

SEXTO.- EUROCEP a fecha de 9 de junio de 2009, mantiene los datos personales del denunciante en sus sistemas, tal como acredita mediante copia de captura de pantalla

de sus ficheros. Consta asociado a los datos personales del denunciante una marca en un campo del sistema denominado Borrar LPD. (Folios 66 y 67)
TERCERO: Centro Organizado de Enseñanza a Distancia S.L. ha presentado en fecha 7 de octubre de 2009 en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en: **Indefensión por haberse producido en la resolución que se recurre una modificación fáctica y jurídica sustancial en relación con el contenido de la propuesta de resolución previa.**
No es cierto el contenido del primer párrafo del antecedente segundo, porque no se ha hecho ninguna solicitud de información a Euroenseñanzas de Formación Profesional, S.L.
En la resolución se dice que *" en el presente caso estamos ante un tratamiento de datos personales del denunciante que CODED (en adelante EUROCEP) gestiona*" la resolución no asume en definitiva la conclusión de la propuesta en el sentido de que no encontramos ante una misa entidad, sino que ahora dice que CODED es EUROCEP, si la propuesta recoge que no encontramos ante una misma entidad, y si siempre hasta el momento se identifico a EUROCEP con la otra sociedad, variar dicha constancia fáctica supone incurrir en falta de claridad que nos deja indefensos.
El escrito de alegaciones a la propuesta se presento en plazo, es decir el día 27 de julio de 2009, para lo cual se aporta copia del justificante de correos.
Si el acuerdo de inicio señala como presuntos responsables a dos sociedades distintas, a ambas debieron notificarse los actos producidos y ello sin olvidar, que, además en la propuesta debió amen de considerarse responsable a una sola de ellas, efectuar declaración del por qué se eximia a la otra, extremo este que no se hizo.
La resolución señala que no obsta que una vez iniciado el procedimiento consta las dos entidades, se proponga sanción solamente contra una de ellas, conclusión que esta parte entiende siempre que a la otra se le hubieran notificado todos y cada uno de los actos producidos hasta el momento.

-Falta de prueba de cargo. Si en los hechos probados se dice que fue EUROCEP la implicada, no puede condenarse a esta parte. De la lectura de la resolución, no puede sacarse más conclusión de que no consta que fuera esta sociedad la que remitió el envío, no siendo óbice para ello.
-Aplicación del art. 45.5 LOPD. En el procedimiento PS 382/2007 se aplico el citado precepto en atención a la implementación de determinadas medidas, mientras que en el FJ VI de la resolución, se reconoce que los datos del denunciante estaban bloqueados.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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 (en lo sucesivo LRJPAC).

II

Con carácter previo a la valoración del fondo del asunto planteado por el recurrente, es necesario de un lado, analizar las cuestiones formales planteadas y de otro aclarar la lógica procedimental del procedimiento sancionador, y la vinculación existente entre la propuesta de resolución y la resolución definitiva.

En lo referente al vencimiento del plazo para formular alegaciones a la propuesta de resolución, esta Agencia no puede hacer otra cosa que reconocer la procedencia de la presentación en plazo de dichas alegaciones, ya que el recurrente ha acreditado documentalmente que presentó en tiempo y forma dichas alegaciones. Ahora bien, la practica habitual de la Sociedad Estatal de Correos y Telégrafos es estampar el sello de la Oficina junto con la fecha, tanto en el sobre como en el escrito en cuestión, (tal como se ha realizado con la presentación del presente recurso), circunstancia que no se produjo en las alegaciones presentadas a la propuesta de resolución, que no tenían dicho sello, ni en el propio documento ni en el sobre, desconociendo esta Agencia, si tal ausencia se debió a la inobservancia del personal de dicha sociedad de correos, o simplemente a que el hoy recurrente presento el sobre ya cerrado, sin que aquel pudiera estampar dicho sello. Por lo que el órgano instructor, con la información que manejaba (solamente tenía como referencia temporal en cuanto a la presentación del escrito, el sello de entrada del Registro de esta Agencia, que databa del 29 de junio de 2009) actuó correctamente.

No obstante lo anterior, el recurrente puede y así lo ha realizado, formular dichas alegaciones en esta vía de recurso.

En lo referente a la vinculación entre la propuesta de resolución y la resolución definitiva, hay que señalar que la propuesta de resolución concreta unos hechos y unos responsables del ilícito administrativo, lo que no vincula de manera plena al órgano que le compete resolver.

Tanto es que la resolución puede incluso es recoger hechos distintos a los acreditados durante la instrucción, tal como legitima el art. 20.1 del Real Decreto 1389/1993, de 4 de Agosto, por el que se aprueba el Reglamento del ejercicio de la potestad sancionadora, que señala que "*en la resolución no se podrán aceptar hechos distintos de los determinados en la fase de instrucción del procedimiento,* ***salvo los que resulten, en su caso, de la aplicación de lo previsto en el número 1 de este artículo, con independencia de su diferente valoración jurídica***." circunstancia que en el presente caso no ha ocurrido tal como puede comprobar el recurrente si compara el apartado de HECHOS PROBADOS de ambos actos administrativos (Propuesta y Resolución).

En cuanto a la fundamentación jurídica, tal como se ha señalado, se permite variar la calificación jurídica, tanto es, que incluso permite variar la gravedad de la sanción a imponer, sin perjuicio del traslado de nuevo al imputado para hacer las alegaciones que estime conveniente, ex art. 20.3 último párrafo.

Por lo que en el presente caso, en nada ha variado ni los hechos probados, ni la calificación jurídica de los mismos, aun estando esta Agencia posibilitada reglamentariamente para ello.

En cuanto a la indefensión alegada por el recurrente, a pesar de la extraordinaria amplitud de aplicación de las garantías del proceso penal reconocidas en el art. 24 de la CE al procedimiento administrativo sancionador, el propio Tribunal Constitucional, en su Sentencia 97/1995 de 20 de junio declara que "*tal aplicación no puede ser literal e inmediata, lo que impide una traslación mimética de las garantías propias del procedimiento judicial al administrativo sancionador en razón a la distinta naturaleza de cada uno de ellos, no obstante la común identidad de ser manifestación del ordenamiento punitivo del Estado*". De esta forma tanto el Tribunal Supremo como el Tribunal Constitucional han venido reconociendo que, en la mayoría de los casos, la mera infracción, en el procedimiento administrativo sancionador, de las garantías procedímentales reconocidas en el art. 24 CE no supone *per se* la anulación o invalidación del procedimiento administrativo o de su resolución sancionadora, (tal como pretende el recurrente, por la variación acaecida a su juicio de la fundamentación fáctico-jurídica de la resolución respecto de la propuesta explicada *ut supra* e inexistente).

Buen ejemplo de la doctrina expuesta, es la Sentencia del Tribunal Supremo de 9 de junio de 1995:" *en modo alguno puede aceptarse que se haya producido indefensión para la parte que nunca quedó privada de formular alegaciones que convino a su defensa, y ello tanto en el expediente administrativo como en el proceso*". *] y 76/1990 [], esta última de aplicación en el caso de las actas de Inspección).* (El subrayado es de la Agencia Española de Proteccion de Datos). (El subrayado es de la Agencia Española de Proteccion de Datos). Así como la Sentencia de 4 de marzo de 1997 que señala que: "*En relación a la pretendida indefensión que alega la empresa sancionada en la vía administrativa, hay que señalar, en primer lugar, que en relación con los expedientes administrativos sancionadores, por su similitud sustancial con el proceso penal, y a diferencia de otro tipo de expedientes administrativos, la jurisprudencia constitucional y la de este Tribunal Supremo viene admitiendo la aplicación del artículo 24 de la CE y la necesidad de ajustar al mismo su tramitación, y ello tiene que ver con las posibilidades de defensa en el expediente, con la contradicción en él, con la posibilidad de presentación de pruebas y con la fundamentación de la resolución sancionadora, únicos elementos a analizar en el proceso desde la perspectiva del referido precepto constitucional (SSTC números 66/1984 [RTC 1984\66], 98/1989 [RTC 1989\98RTC 1990\76*

Dicho lo anterior, en cuanto a la indefensión alegada por el recurrente, la jurisprudencia de la Audiencia Nacional y del Alto Tribunal, ha señalado que ésta debe ser una verdadera indefensión material, esto, es que la misma haya originado un menoscabo real de su derecho de defensa causándole un perjuicio real y efectivo (SSTC 155/1998,212/1994,137/1996,89/1997) y en el presente caso la recurrente pretende entender producida la indefensión por la no justificación de la exención de responsabilidad a la otra entidad imputada inicialmente.

A este respecto señalar que en ningún caso tal exención conlleva la indefensión de la hoy recurrente, cuando se han observado las garantías procedímentales, (y tal como recoge la jurisprudencia citada "*nunca quedó privada de formular alegaciones que convino a su defensa, y ello tanto en el expediente administrativo como en el proceso"* y "*las posibilidades de defensa en el expediente, con la contradicción en él, con la posibilidad de presentación de pruebas y con la fundamentación de la resolución sancionadora, únicos elementos a analizar en el proceso desde la perspectiva del referido precepto constitucional")*, máxime cuando en vía de recurso administrativo y contencioso-administrativo puede hacer valer sus pretensiones, tal como esta realizando en la presente instancia administrativa.

Asimismo, en el mismo orden de cosas, la recurrente alega que "*La resolución señala, penúltimo párrafo FJ III, que, no obsta que una vez iniciado el procedimiento contra las dos entidades, se proponga sanción solamente contra una de ellas, conclusión que esta parte entiende siempre que a la otra se le hubieran notificado todos y cada uno de los actos producidos hasta el momento*."

Tal afirmación es del todo ilógica y carente de fundamento jurídico, ya que el órgano instructor no esta sujeto a otro mandato que, sin perjuicio de lo establecido en las Constitución y las leyes vigentes, al del propio RD 1389/1993, de 4 de agosto, por lo que dejar de imputar a una entidad contra la que inicialmente se dirigió el acuerdo de inicio, es del todo licito, sin que sea relevante que le hayan solicitado información o no, y que se la hayan notificado el resto de actos administrativos o no. En cuanto a la confusión alegada por la recurrente entre su denominación y la de la otra entidad denunciada, señalar que tal confusión es inexistente, ya que tanto en la propuesta de resolución, como en la resolución recurrida, se denomina a la imputada como EUROCEP (folio 73 y página 5/12 de la resolución), con independencia de que dentro de tal denominación en la Resolución, se excluya a la otra entidad inicialmente imputada y que consta en la propuesta de resolución. Es decir en nada se ha variado la imputación realizada a la recurrente durante todo el procedimiento.

En definitiva, no es posible pretender que al socaire de una confusión inexistente entre la denominación de las entidades inicialmente imputadas, se cree una zona de impunidad para el recurrente, cuando de conformidad con lo expuesto en el Fundamento de Derecho III (tal como se expondrá a continuación) , hay elementos suficientes para definir la identidad y personalidad jurídica de la infractora, hoy recurrente.

III

En segundo lugar, la recurrente alega la falta de prueba de cargo suficiente para enervar la presunción de inocencia. Dicha alegación ha de ser desestimada, ya que la resolución en su Fundamento de Derecho III, analiza los elementos de juicio acreditados para tener por consumada la infracción por parte de la recurrente, tal como se transcribe a continuación:

"Pues bien, en primer lugar, la referencia a EUROCEP en el procedimiento, lo es para evitar referencias extensas que han de repetirse en el texto de la propuesta de resolución, siendo su referencia hecha a Centro Organizado de Enseñanza a Distancia S.L, con independencia de que se entienda desde esta Agencia que ambas entidades están especialmente vinculadas.

En segundo lugar, es necesario clarificar que respecto de Centro Organizado de Enseñanza a Distancia S.L, se ha acreditado que es la titular del dominio de eurocep.es, que es el que aparece en los envíos publicitarios y ante quien ejercer los derechos ARCO (reverso del folio 5, que señala que "la información utilizada en este envió pertenece al fichero general de EUROCEP. Usted podrá ejercer su derecho de acceso, rectificación o cancelación de sus datos."). Lo que no ofrece ninguna duda de que estamos ante la entidad imputada.

En tercer lugar, en el folio 67, se acredita que Centro Organizado de Enseñanza a Distancia S.L, tiene los datos del denunciante, sin acreditar el origen licito de los mismos, ya que se limita a manifestar que los proporcionó el propio denunciante, sin acreditar tal extremo. Asimismo en el folio 25 del procedimiento asume la recepción de una solicitud de cancelación de datos por parte del denunciante y el acaecimiento de un error en su gestión, lo que se muestra suficiente para tener por consumada la infracción del art. 16 de la LOPD por parte de Centro Organizado de Enseñanza a Distancia S.L. desconociendo esta Agencia, en base a qué entiende la entidad denunciada que se ha producido indefensión ya que la participación en los hechos constitutivos de infracción grave a la LOPD por parte de Centro Organizado de Enseñanza a Distancia S.L, es de tal claridad que no ofrece ninguna duda, esto es, ante ella se ejerce un derecho de cancelación, tal como reconoce, y con posterioridad se le envía publicidad utilizando sus datos, lo que evidencia que no se atendió a dicho ejercicio.

En cuarto y ultimo lugar, en el ya citado folio 25 del procedimiento Centro Organizado de Enseñanza a Distancia S.L., reconoce que el fichero utilizado para el envío es el denominado PUBLICIDAD inscrito en el Registro General de Protección de Datos, con el número XXXXXX/XXXX. a este respecto aclarar que dicho número no es el del registro en si, sino el número de referencia de entrada.

Consultado el RGPD se ha obtenido que el fichero inscrito con código ########, con número de entrada XXXXXX/XXXX y denominado PUBLICIDAD, (folio 86) su titularidad corresponde a Centro Organizado de Enseñanza a Distancia S.L., lo que despeja toda duda a cerca de la participación de la citada entidad en la no cancelación de datos y en el ulterior envío publicitario."

IV

Finalmente, la recurrente solicita la aplicación el art. 45.5 de la LOPD, en base a su aplicación en el procedimiento PS/386/2007. A este respecto, señalar que en dicho procedimiento se acreditaron la implantación de medidas tendentes a la no producción de ninguna otra vulneración de la normativa de proteccion de datos que junto con las circunstancias concretas del caso permitió la aplicación del citado precepto. En el presente caso nada de esto ha ocurrido, la referencia que se hace en el hecho probado Sexto de la resolución, en nada puede asemejarse a la implementación de medidas tendentes al cumplimiento de la LOPD, ya que precisamente de la actuación de la recurrente se infiere que no cumplió los preceptos de la norma, tal como fue

analizada y desestimas en el Fundamento de Derecho VIII, tal como se transcribe a continuación:

<<“ *Los hechos fundamentales acaecidos en el presente supuesto se centran en la no cancelación efectiva de los datos personales del denunciante a pesar de haber solicitado éste su cancelación y la entidad confirmarla. La legitimación de la denunciada para la constancia de los datos del denunciante en sus sistemas, no se ha acreditado, manifestando EUROCEP que su constancia se debía a una llamada del denunciante, sin que guarden prueba de dicha circunstancia; asimismo la constancia de una marca en los datos del denunciante que referenciar un bloqueo para actividades de prospección comercial, no ha resultado efectiva, dado que los datos del denunciante se sometieron a posterior tratamiento, sin que la entidad haya acreditado el motivo del error en sus sistemas y la solución propuesta para que tal “error” no se vuelva a producir. Lo que supone una falta de diligencia en su actuación y ninguna evidencia que haya presumir implantación de algún tipo de medida o mejora que haga que los hechos valorados no se vuelvan a producir.*

La diligencia exigible nos la da la profesionalidad del infractor, es decir, la actividad a la que se dedica, por lo que ésta debe ser mayor cuando, precisamente, se maneja un gran número de datos personales. Así lo han recogido la Sentencia de la Audiencia Nacional de Recurso 104/2006 señala que “la entidad demandante por la actividad que realiza debe tratar un gran volumen de datos personales en sus ficheros, lo que hace que deba extremar el cuidado en el manejo de dichos datos para lograr una proteccion eficaz, pues está en juego un derecho fundamental autónomo, el derecho a la proteccion de datos personales según la STS 292/2000”.

En el mismo sentido la Sentencia de la Audiencia Nacional, Recurso 143/2006 señala que” así es, no se aprecia la disminución de la culpabilidad del sancionado o de la antijuridicidad del hecho, pues la naturaleza de la actividad desarrollada por la entidad recurrente, y su permanente relación con los datos personales, determina que el comportamiento exigible a quien habitualmente está en contacto con este tipo de datos sea de distinguido y exquisito cuidado sobre el cumplimiento de las exigencias impuestas por la LOPD, porque está en juego la proteccion de derechos fundamentales- art. 18.4 CE-. “

Por su parte, el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible, y en la valoración del grado de dicha diligencia, ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda que, en el caso ahora examinado, cuando la actividad de EUROCEP de constante y abundante manejo de de datos, ha de insistirse en el rigor y el exquisito cuidado para ajustarse a las prevenciones legales al respecto (STS de 5 de junio de 1998).

En el presente caso estamos ante una grave falta de diligencia, en tanto que EUROCEP, marcó los datos del denunciante en su fichero de clientes para no ser tratados con finalidades de prospección comercial, pero dicha marca no funcionó siendo utilizados los datos para dicha finalidad. En definitiva, estamos ante una entidad que maneja gran volumen de datos personales, y acontece una grave falta de diligencia, así las cosas, pierde efectividad y existencia lógica cualquier tipo de marca en los ficheros de EUROCEP que tiendan a su bloqueo, ya que si no se gestiona bien, el resultado es como no realizar ninguna marca en sus ficheros, ni atender derechos de los titulares de datos personales. Sin que se hayan puesto de manifiesto circunstancias que permitan la aplicación del citado art. 45.5 LOPD.

Respecto de los criterios de graduación de las sanciones del art. 45.4 de la LOPD, y en atención a la falta de intencionalidad, se propone la sanción en su cuantía mínima.>>>

Respecto a la no acreditación del volumen de datos que maneja la recurrente, hay que estimar dicha alegación ya que no se ha practicado prueba de cargo que verifique

dicho extremo. No obstante, de la actividad mercantil a la que se dedica, se infiere un continuo tratamiento de datos, lo que impide, con independencia del volumen de los mismos, aplicar el citado precepto.

V

Por lo tanto, en el presente recurso de reposición, Centro Organizado de Enseñanza a Distancia S.L. no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por Centro Organizado de Enseñanza a Distancia S.L. contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 7 de septiembre de 2009, en el procedimiento sancionador PS/00219/2009.

SEGUNDO: NOTIFICAR la presente resolución a la entidad Centro Organizado de Enseñanza a Distancia S.L.

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, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

Procedimiento nº.: PS/00328/2005

ASUNTO: Recurso de Reposición
Examinado el recurso de reposición interpuesto por la entidad **CENTRO DE ESTUDIOS CEAC, S.L.** contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00328/2005, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 04/07/2006, se dictó resolución por el Director de la Agencia Española de Protección de Datos en el procedimiento sancionador PS/00328/2005, en virtud de la cual se imponía a la entidad **CENTRO DE ESTUDIOS CEAC, S.L.** (en lo sucesivo Ceac), una sanción de 300.506,05 € (trescientos mil quinientos seis euros con cinco céntimos de euro) por vulneración de lo dispuesto en el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), infracción tipificada como muy grave en el artículo 44.4.b), de conformidad con lo establecido en el artículo 45.3 y 4 de la citada Ley Orgánica.
Dicha resolución, que fue notificada al recurrente en fecha 06/07/2006, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en los artículos 18 y 19 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor según lo establecido en la disposición transitoria tercera de la LOPD.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00328/2005, quedó constancia de los siguientes:
<<PRIMERO: Los datos de D. J.B.S. figuran en las "Páginas Blancas", accesibles a través de Internet, sin embargo en esta publicación no consta el piso y la puerta que sí aparecen en la dirección postal a la que se dirigió el envío publicitario de Arcadia (folio 7).
SEGUNDO: D. J.B.S. facilitó, en fecha 21/11/2003, a Ceac sus datos personales, al solicitar información sobre un curso de Técnico de Gestión Medioambiental, a través de su página web, en la que se incluye un "formulario de solicitud de información" sobre los cursos que ofrecen.
En el citado formulario de recogida de datos de Ceac, figuraba la siguiente información "Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de Centro de Estudios CEAC, S.L. para gestionar la relación comercial con usted. Usted tiene los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía:(C/.....). Es posible que en un futuro –incluso finalizada nuestra relación comercial- utilicemos sus datos personales para informarle sobre nuestros productos y/o servicios o que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollen su actividad en los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, con el fin de que le informen sobre los productos o servicios que comercialicen" (folio 213). El subrayado recoge el contenido de la cláusula que difiere de la sometida a informe del Gabinete Jurídico de la Agencia, que se recoge en el Hecho Probado Sexto que más adelante se transcribe.
TERCERO: En septiembre de 2004, D. J.B.S. recibió por correo postal una información comercial de la compañía Arcadia, estando en desacuerdo con el procedimiento utilizado por esta compañía para obtener sus datos personales. En el mismo se informa que "El listado de direcciones utilizado para la realización de esta

campaña publicitaria ha sido elaborado por la entidad Arvato Services Iberia, S.A. ((C/.....), Teléfono #######), a la que usted puede dirigirse a fin de ejercer sus derechos de acceso, rectificación, cancelación y oposición", previsto para los casos en los que los datos no procedan del "fichero BDT" cuyo responsable es Arvato (folios 1 a 4).

CUARTO: La compañía que figura en el envío publicitario, Arcadia, ha manifestado que los datos utilizados para el citado "mailing", realizado en septiembre de 2004, les fueron facilitados por Arvato según consta en el lateral de la comunicación recibida por el denunciante, cuyo tenor literal se ha recogido en el Hecho Probado anterior. Asimismo, manifiesta que los datos relativos al denunciante no se han incluido en los ficheros de la entidad Arcadia, dado que, al no interesarse en los productos promocionados, no llegó a ser cliente suyo. Arvato y Arcadia suscribieron un contrato el 3/01/2000, por el que aquélla encomienda a Arvato la elaboración de un listado de destinatarios o de una campaña o acción publicitaria, para lo cual podrá utilizar sus propios ficheros o los de terceras personas o entidades con las que Arvato firme contratos de "listbroking".

Arvato ha remitido diversas facturas emitidas por los servicios que presta a Arcadia (folios 11- 12, 31 – 38, 42 - 44, 39 - 41). En las diversas facturas, remitidas por Arvato a esta Agencia Española de Protección de Datos en relación con los servicios prestados por la misma a la entidad Arcadia, consta claramente que es esta entidad, Arvato, quien realiza la facturación y el cobro de los servicios prestados, haciendo sólo en la descripción, una referencia a los ficheros de los que se han obtenido los datos.

QUINTO: En el contrato de 2/12/2003, suscrito entre Arvato y Ceac, se informa que los datos utilizados para elaborar el listado de destinatarios de la campaña publicitaria de Arcadia, recibida por el denunciante, proceden del fichero que le facilitó la entidad Ceac, con quien ha suscrito el citado contrato de "listbroking".

En el citado contrato, apartado II, se manifiesta que "ARVATO dispone, para su actividad, de los más variados contactos con empresas para las que desarrolla campañas de publicidad directa mediante el tratamiento automatizado de listas de nombres...A los efectos de este contrato, tales empresas se referirán como los <<CLIENTES>>" (folio 47).

A lo largo del texto del citado contrato, apartado V, se establece lo siguiente:

"Que, con independencia de los acuerdos o pactos que ARVATO pueda tener establecidos con"...(en este caso, Ceac)..."de forma previa a su tratamiento y utilización para cualquier campaña encargada por un CLIENTE..." (en este caso, Arcadia)..."procede a recabar la oportuna aprobación por escrito del TITULAR DEL FICHERO"...(en este caso, Ceac)..."respecto del encargo de que, en cada caso, se trate" (folio 48).

El TITULAR DEL FICHERO ...(en este caso, Ceac)..."manifiesta que ha recabado el consentimiento de las personas cuyos datos personales obran en el fichero"...(en este caso el "Fichero Maestro de Promociones", de Ceac)..."para que sus datos personales sean utilizados para fines publicitarios por empresas que desarrollan su actividad en los sectores de telecomunicaciones, financiero, ocio, formación, gran consumo, automoción, energía, agua, y ONG" (pacto primero, párrafo tercero del mencionado contrato) (folio 49).

"ARVATO está autorizada para representar al TITULAR DEL FICHERO"...(en este caso Ceac)..."en la negociación de los contratos con los CLIENTES"...(en este caso, con Arcadia)..."A estos efectos, actuará en nombre y por cuenta del TITULAR DEL FICHERO" (Ceac), (pacto segundo del contrato) (folio 50).

"Con la firma de este contrato el TITULAR DEL FICHERO"...(en este caso, Ceac)..."facilita a ARVATO una copia completa y actualizada del fichero"...(en este caso "Fichero Maestro de Promociones"..."en soporte informático para su más ágil tratamiento en las instalaciones de ARVATO"..."la entrega del mismo tiene un mero

carácter instrumental...sin que ello suponga, en ningún caso, ...alteración ...ni modificación de carácter del TITULAR DEL FICHERO o su responsabilidad sobre el fichero" (pacto cuarto, párrafos primero y segundo) (folio 50).
"EL TITULAR DEL FICHERO percibirá las contraprestaciones que se fijen..." "ARVATO percibirá por los servicios prestados al TITULAR DEL FICHERO las contraprestaciones indicadas en el anexo..." (pacto séptimo del citado contrato) (folio 52).
Por lo que se refiere a las "condiciones económicas", de "facturación y pago" y de "contraprestaciones del Agente", el Anexo al contrato de 2/12/2003 dispone que Ceac, como TITULAR DEL FICHERO, percibirá las contraprestaciones en función de la utilización de las direcciones realizada por ARVATO, expidiendo la correspondiente factura a la fecha de confirmación que le haga ARVATO que, como agente, percibirá una comisión que se deducirá de la factura expedida por Ceac (Anexo al contrato en folios 56-58).
SEXTO: El Grupo Planeta, al que pertenece Ceac, sometió a informe del Gabinete Jurídico de la Agencia Española de Protección de Datos, la siguiente cláusula informativa que difiere de la implementada por la citada entidad, en este caso, para la recogida de datos del denunciante. Dicha cláusula tenía el siguiente tenor literal:
<< Los datos personales que usted nos facilita serán incluidos en el fichero automatizado de_____, S.A. para gestionar la relación comercial con usted. Usted podrá ejercer los derechos de acceso, cancelación, rectificación y oposición, que podrá ejercitar mediante carta dirigida a esta compañía Calle ,_____. Del mismo modo, Ud. consiente a que en un futuro -incluso finalizada nuestra relación comercial -_____, S.A. utilice sus datos personales para informarle sobre sus productos y/o servicios y a que comunique tales datos a otras empresas del Grupo Planeta cuyas actividades se relacionen con los sectores editorial, de formación, de cultura y de ocio, con el fin de que le informen sobre los productos o servicios que comercialicen. Si no desea ser informado de nuestros productos o servicios o de los de otras empresas del Grupo Planeta, indíquenoslo por escrito en la dirección arriba indicada, señalando claramente su nombre, apellidos y dirección o hágalo constar en este cupón, marcando la siguiente casilla □ (Ley Orgánica 15/1999 de 13 de Diciembre).>>" (folio 193). >>

TERCERO: Por la parte recurrente se ha presentado con fecha de entrada en esta Agencia Española de Protección de Datos de 20/07/2006, recurso de reposición fundamentándolo, básicamente, en las mismas alegaciones ya efectuadas a lo largo del procedimiento sancionador PS/00328/2005, insistiendo en la aplicación de lo establecido en el artículo 45.5 de la LOPD, en base a las medidas adoptadas para que no se vuelva a producir una situación como la que dio lugar a la resolución recurrida.
Así mismo alegan y acreditan, la conducta diligente que han tenido en aplicar lo dispuesto en el artículo 5.1 a) de la mencionada Ley Orgánica, incluyendo las recomendaciones del Director de la Agencia , dictadas en el año 2001, para redactar la cláusula informativa, y modificándolas de acuerdo con el criterio del Gabinete Jurídico de 12 de julio de 2004.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto 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.

II

En relación con las manifestaciones efectuadas por Ceac, reiterándose en las alegaciones ya presentadas a lo largo del procedimiento sancionador e insistiendo en la adecuación de sus actuaciones a la normativa de protección de datos, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho del II al VII, ambos inclusive, XI, XII y XIII de la Resolución recurrida, R/00457/2006, de 4/07/2006, tal como se transcribe a continuación:

"II
De los antecedentes y hechos probados señalados con anterioridad, se deducen dos cuestiones de fondo. La primera, si cabe deducir que Ceac obtuvo, en el momento de la recogida de los datos, a través del formulario incluido en su página web, el consentimiento inequívoco del denunciante de modo que se encontrara habilitada para su cesión a terceros sin consentimiento del mismo, y, la segunda, si la entidad Arvato ha actuado en el presente supuesto como encargado de tratamiento de Ceac, en virtud del contrato suscrito por ambas entidades el 2/12/2003.
III
Respecto a la primera cuestión el artículo 5 de la LOPD, dispone lo siguiente:
"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos . d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una Ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo

autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten."
De acuerdo con lo establecido en el citado artículo 5 de la LOPD, el responsable del fichero debe informar, en el momento de la recogida de los datos, de los extremos establecidos en el citado artículo. La información a la que se refiere el citado artículo debe suministrarse a los afectados previamente a la recogida de sus datos personales, y deberá ser expresa, precisa e inequívoca.
El número 2 del mismo precepto establece una regla especial para los supuestos en que se utilicen cuestionarios u otros impresos para la recogida de los datos, exigiendo que "figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior."
La LOPD ha querido, por tanto, imponer una formalidad específica en la recogida de datos a través de cuestionarios u otros impresos, que garantice el derecho a la información de los afectados. A tal efecto, impone la obligación de que la información figure en los propios cuestionarios o impresos, y la refuerza exigiendo que conste de forma claramente legible.
IV
La Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, que delimita el contenido esencial del derecho fundamental a la protección de los datos personales, se ha pronunciado sobre la importante vinculación entre el consentimiento y la finalidad para el tratamiento de los datos personales, en los siguientes términos: " el derecho a consentir la recogida y el tratamiento de los datos personales (art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con éstos (art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por ley, pues el derecho fundamental a la protección de datos personales no admite otros límites.
De otro lado, es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia" (el subrayado es de la Agencia Española de Protección de Datos).
De lo expuesto cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales en lo relativo a los requisitos del consentimiento, de la información previa a éste, y de las finalidades para las que los datos pueden ser recabados y tratados.

Asimismo, la citada Sentencia 292/2000, ha considerado el derecho de información como un elemento indispensable del derecho fundamental a la protección de datos al declarar que "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y, el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que rectifique o los cancele." (el subrayado es de la Agencia Española de Protección de Datos).

V

Ceac en las alegaciones a la propuesta de resolución señala que la cláusula informativa que implementó en la página web, en el momento de la recogida de los datos, es suficiente para acreditar un consentimiento inequívoco del denunciante, haciendo referencia a que esta Agencia siempre ha entendido suficiente la enumeración de los sectores de actividad a los cuales se haría cesión de los datos. Frente a dicha alegación, ha quedado acreditado en el presente procedimiento sancionador, y así ha sido reconocido por Ceac, que dicha entidad se separó del informe emitido por el Gabinete Jurídico de esta Agencia, señalando que nunca ha defendido la identidad de leyendas, sino la identidad de criterios contenidos en ambas leyendas. Dicha alegación no puede ser compartida por esta Agencia ya que la cláusula finalmente aplicada por Ceac recogía diferencias sustanciales de las cuales se deducía la recogida de un consentimiento no inequívoco por parte de los interesados.

De acuerdo con lo señalado, en el presente caso, consta acreditado que Ceac ha venido utilizando una cláusula informativa, en el momento de la recogida de los datos a través de su web, que no recoge los extremos a que se refiere el apartado a) del artículo 5.1 de la LOPD, sin que de dicha información se dedujese claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que éstos se recaban.

En relación al citado apartado a) del artículo 5.1, la citada cláusula informativa no concreta de modo expreso, preciso e inequívoco la finalidad de la recogida de los datos y de los destinatarios de la información, ya que las referencias a "los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones", se refiere a términos inconcretos de los que no caben deducir, sin duda o equivocación, la finalidad para la cual van a ser cedidos, lo que impide que el

interesado pueda conocer, como señala el Tribunal Constitucional, "a qué uso lo está destinando y , por otro lado, el poder oponerse a esa posesión y usos".
En este sentido, resultan ejemplificadores dos circunstancias que han concurrido en el presente supuesto:
-- El propio denunciante, que según Ceac había prestado un consentimiento informado, a través de su web al solicitar información sobre un curso el 21/11/2003, sin embargo no pudo asociar que el envío publicitario de Arcadia, en el que se le informaba que el listado de direcciones había sido elaborado por Arvato, sobre el "Fichero Maestro de Promociones" de Ceac, tuviera ninguna relación con la citada recogida de datos.
-- Ceac en el formulario de recogida de datos se refiere a la comunicación a empresas de los sectores financiero, editorial, textil, hogar, belleza, enseñanza, ONG, venta por correo y/o comunicaciones, cuando en el contrato suscrito con Arvato el 2/12/2003 se refiere a los sectores de las telecomunicaciones, financiero, ocio, formación, gran consumo, energía, agua y ONG, existiendo una clara diferencia en cuanto a que en el contrato de 2/12/2003, no se prevé que Ceac le pueda dar acceso a Arvato para fines de venta por correo y/o comunicaciones. Frente a dicha argumentación Ceac señala en las alegaciones a la propuesta que de dicha discordancia no se aprecia qué consecuencia jurídica puede ello acarrear en cuanto a los derechos del denunciante, ya que la relación entre Ceac y Arvato es bilateral y privada, y lo importante no es el contenido de dicha relación sino el de la cláusula informativa que reciba. No puede admitirse dicha alegación, porque el consentimiento inequívoco del denunciante, sobre el que se fundamenta el poder de control y disposición de sus datos, es el que debe limitar los usos y finalidades que, precisamente, pretendan realizarse con los mismos.
A mayor abundamiento, la Audiencia Nacional en Sentencia de 13/04/2005 ya señaló que "la amplitud de categoría de bienes y servios para los que se presta el consentimiento... tampoco permite al particular, identificar de forma determinada y explícita las finalidades para los que serán tratados sus datos personales, en términos que le permitan prestar un conocimiento inequívoco como el exigido por la LOPD".
Tampoco en la cláusula informativa se informa de modo expreso, preciso e inequívoco, sobre los destinatarios de la información, haciéndose una genérica referencia en el siguiente sentido "...que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo..." En este sentido, como más adelante se referirá, la cláusula informativa de Ceac no coincide con la informada por esta Agencia con fecha 7/07/2004, ya que añade de forma inconcreta los destinatarios de los datos al referirlos, en general, a "empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo".
De acuerdo con lo señalado, de la cláusula implementada por Ceac no cabe deducir que el denunciante hubiese prestado su consentimiento inequívoco para el tratamiento de sus datos, y , menos aún, para proceder a ceder sus datos a un tercero. Por lo tanto se considera que Ceac ha vulnerado lo previsto en el artículo 11 de la LOPD, que en su apartado 1, dispone lo siguiente:
"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."
En el supuesto examinado, ha quedado probado que la entidad Ceac es la responsable del "Fichero Maestro de Promociones" del que se obtuvieron los datos del denunciante utilizados para el envío publicitario enviado, sin que haya acreditado que tuviera el consentimiento del denunciante para comunicar sus datos a Arvato, ni estar exceptuada para ello conforme al apartado 2 de dicho precepto.
VI
El artículo 44.4.b) de la LOPD, establece que será infracción muy grave:

" b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas". En el presente caso, ha quedado acreditado que Ceac comunicó los datos del denunciante a Arvato sin que constara el consentimiento inequívoco de éste ya que los términos recogidos en la cláusula informativa, recogida en la web de Ceac, no incluía los extremos a los que se refiere el apartado a) del artículo 5 de la LOPD. En consecuencia, la citada comunicación supone una vulneración del artículo 11 de la LOPD que encuentra su tipificación en el citado artículo 44.4.b) la citada Ley Orgánica.

VII

En cuanto a la segunda cuestión de fondo que se planteaba en el Fundamento de Derecho I de esta Resolución, es decir sobre si, en el presente supuesto, Arvato ha actuado como encargado de tratamiento de Ceac, al amparo del contrato suscrito entre ambas entidades el 2/12/2003, en cuyo caso no debería responder de vulneración alguna de la LOPD pues habría actuado en nombre y por cuenta de Ceac, es preciso recordar que el artículo 12 de la LOPD, al regular el "Acceso a los datos por cuenta de terceros", establece lo siguiente:

"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."

En el presente caso, Ceac en sus alegaciones afirma que no ha realizado una cesión de datos a la entidad Arvato, por cuanto la misma es simplemente un encargado del tratamiento de sus ficheros, en base al contrato de "listbroking" de fecha 2/12/2003, suscrito entre ambas entidades. En relación con dicho asunto, y además de lo señalado en el Fundamento de Derecho anterior, conviene recordar que en los Hechos Probados han quedado acreditados los siguientes extremos:

Ceac manifiesta que ha recabado el consentimiento de los interesados incluidos en el "Fichero Maestro de Promociones".

Ceac está interesada en que Arvato utilice su fichero en las promociones que le encarguen sus clientes, que actúan como beneficiarios de la publicidad.

Ceac facilita una copia completa del fichero a Arvato.

Arvato se compromete, antes de usar el fichero, a pedir autorización a Ceac y se constituye en representante de ésta para negociar los contratos de sus clientes.

Arvato realiza en su nombre los contratos con los beneficiarios de la publicidad y usa, a su juicio, tanto los ficheros propios como los de las entidades con las que ha suscrito un contrato de "listbroking".

Ceac factura a Arvato, según las consultas que ésta le confirma, deduciendo del precio su comisión.

Arvato factura, en su exclusivo nombre, al beneficiario de la publicidad según el contrato establecido al efecto.
Respecto a dicho asunto, en la Sentencia de la Audiencia Nacional, de 29/04/2005, la Sala aplica la siguiente doctrina:
"Se plantea en definitiva a la Sala el problema de la diferenciación entre la cesión y el encargado de tratamiento, "encargado de tratamiento" que no venía expresamente regulado en la LO 5/1992, pero entendía la doctrina que tenía cabida en lo establecido en el Art. 27. Siguiendo lo dispuesto en tal Directiva Europea 95/46/CE, la LO 15/1999 ha regulado específicamente la figura en los aludidos Art. 3.g) y 12, y de hecho la definición de "encargado de tratamiento" contenida en el Art. 3.g) no es sino trascripción del Art. 2.e) de la Directiva.
Y si bien la diferencia entre encargo de tratamiento y cesión, como reconoce la doctrina, en algunos casos es compleja, lo que es evidente es que no puede haber cesión cuando existe encargo de tratamiento y no resulta preciso el consentimiento del afectado.
Lo típico del encargo de tratamiento es que un sujeto externo o ajeno al responsable del fichero va a tratar datos de carácter personal pertenecientes a los tratamientos efectuados por aquél con el objeto dc prestarle un servicio en un ámbito concreto. Habría por tanto encargo de tratamiento en los supuestos de outsourcing o en los de prestación derivada de un contrato de obra o arrendamiento de servicios con un fin concreto. Siendo esencial, para no desnaturalizar la figura, que el encargado del tratamiento se limite a realizar el acto material de tratamiento encargado, y no siendo supuestos de encargo de tratamiento aquellos en los que el objeto del contrato fuese el ejercicio de una función o actividad independiente del encargo..."
"En definitiva xxx y xxxx accedieron a los datos personales del afectado, para prestar un servicio, más no a la cesionaria de tales datos, sino a las beneficiarias de la obtención de los mismos, por lo que de ningún modo su relación con xxx puede ser considerada como un encargado de tratamiento a tenor del art. 12 de la LOPD, y tal pretensión ha de ser desestimada."(el subrayado es de la Agencia Española de Protección de Datos).
Asimismo otras sentencias de la Audiencia Nacional, también han tenido ocasión de referirse a esta cuestión:
En la Sentencia de 24/06/2003, la Sala ante un supuesto de pretendido contrato de arrendamiento de servicios por cuenta de tercero, que, a juicio del cesionario, le eximía de solicitar el consentimiento de los afectados, señaló que no se trataba de una auténtica prestación de servicios por cuenta de terceros porque para ello el tercero se debería de haber limitado a efectuar el tratamiento por cuenta del responsable, pero ello no fue así porque el tercero... "no desaparece de la relación, sino que utiliza los datos en su provecho económico...", cuando lo que debería ser es que el tercero recibiera su remuneración del responsable del fichero por cuenta del que trata sus datos.
En la Sentencia de 15/10/2004, reitera la doctrina anterior al señalar que no son incardinables en el artículo 12 de la LOPD, los supuestos en los que el tercero no actúa como encargado de tratamiento porque... "no es encargado...en los términos previstos en el artículo 3.g) de la Ley 15/1999 (por cuanto no trata los datos personales por cuenta del responsable del tratamiento, sino en beneficio propio)..."
De acuerdo con la doctrina señalada, no cabe deducir que del contrato suscrito entre Arvato y Ceac de 2/12/2003, aquélla se constituyera en encargado de tratamiento de ésta ya que ha quedado acreditado que Arvato actuó, en todo momento, ejecutando un contrato suscrito con el beneficiario de la publicidad, es decir, en beneficio propio, facturando a éste y confirmando a Ceac los datos obtenidos de sus ficheros para descontar su comisión por la actividad desarrollada por su cuenta.>>
<<XI

No pueden ser tenidas en cuenta las alegaciones de Ceac, en el sentido de que su cláusula informativa había sido informada favorablemente por esta Agencia Española de Protección de Datos, por cuanto que, como ya se ha señalado, la cláusula utilizada para la recogida de datos del denunciante, se recogía "... que comuniquemos tales datos a las empresas que integran el grupo mercantil Planeta, así como a otras empresas asociadas a la Federación Española de Comercio Electrónico y Marketing Directo que desarrollen su actividad en los sectores...", y no se corresponde con la informada por la Agencia por cuanto en la primera se establecía que "...a que comunique tales datos a otras empresas del Grupo Planeta cuyas actividades se relacionen..."

XII

Por otro lado, el artículo 49 de la LOPD señala: "En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido la Agencia Española de Protección de Datos podrá., mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas."

XIII

De acuerdo con lo establecido en el artículo 45.2, 3, 4 y 5 de la LOPD:

"2. Las infracciones graves serán sancionadas con multa de 60.101,21 € a 300.506,05 €."

"3. las infracciones muy graves serán sancionada con multa de 300.506,05 € a 601.012, 10 €"

"4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora."

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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."

La aplicación con carácter excepcional del citado artículo 45.5 exige la concurrencia de, al menos, uno de los siguientes requisitos: a) Disminución de la culpabilidad del imputado y b) Disminución de la antijuricidad del hecho.

Durante la tramitación del presente procedimiento, ha quedado acreditado que Arcadia actuó en la creencia de que al no tratar en ningún momento datos de carácter personal, en ningún caso su conducta podría vulnerar, como así ha sido, el artículo 6 de la LOPD. En relación a este asunto, como mayor garantía, contrató con Arvato la promoción de la campaña publicitaria que ha dado lugar al presente procedimiento sancionador. En consecuencia se considera que concurre una disminución cualificada de la culpabilidad que permite aplicar a Arcadia el artículo 45.5 de la LOPD.

En el caso de Ceac, ha quedado acreditado, como asimismo dicha entidad reconoce, que se apartó de la cláusula informativa que había sido sometida a informe del Gabinete Jurídico de esta Agencia, deduciéndose de la finalmente implementada diferencias sustanciales que permiten deducir que los interesados no prestaron su

consentimiento inequívoco para la comunicación de sus datos con fines publicitarios. Por dicho motivo, no se observan motivos que permitan aplicar, en el presente supuesto, el artículo 45.5 a la citada entidad.
Asimismo, en relación a los criterios de graduación de las sanciones recogidos en el artículo 45.4 de la LOPD, y en especial, en función de la ausencia de intencionalidad y de reincidencia acreditadas a lo largo del presente procedimiento, procede imponer a la entidad Arvato una sanción de 60.101,21 €, a la entidad Arcadia una sanción de 6.000 €, y a la entidad Ceac una sanción de 300.506,05 €".

III

La alegación principal en la que Ceac fundamenta el presente recurso es la aplicación de lo dispuesto en el artículo 45.5 de la LOPD, basándolo, principalmente, en que ha sido diligente para ir modificando la cláusula informativa del artículo 5 de la LOPD de acuerdo a los criterios de la propia Agencia Española de Protección de Datos, y a que se prohibieron todas las acciones que implicaran la comunicación de datos de Ceac a entidades ajenas al Grupo Planeta.
Asimismo en relación a los criterios de Graduación de las sanciones recogidos en el artículo 45.4 de la LOPD, y , en especial, en función de la ausencia de intencionalidad y de reincidencia acreditadas en el procedimiento, procede imponer una sanción de 60.101,21 €.
El artículo 45.5 de la LOPD establece*: " Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, 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 relación con la aplicación del artículo 45.5 de la LOPD, la Audiencia Nacional ha señalado, entre otras, en Sentencia de 27/10/2004, que *"el citado precepto concreta el principio de proporcionalidad (reconocido para el Derecho administrativo sancionador, con carácter general, en el art. 131.3 de la Ley 30/1992), permitiéndose la disminución en un grado de la sanción aplicable en casos de cualificada disminución de la culpa o de la antijuridicidad. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y sólo en casos en los que la culpabilidad y la antijuridicidad resulten sustancialmente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor de justicia (art. 1.1 CE), por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos. Pues bien, en el caso de autos, la Sala entiende que dicho precepto no es de aplicación porque a la antijuridicidad no obsta la falta de intención de infringir las normas jurídicas (Sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de 4 de junio de 1999), y ya hemos razonado la falta de diligencia de la entidad recurrente".*
En relación a la alegación planteada por Ceac respecto a que resultaría aplicable el artículo 45.5 de la LOPD en cuanto que ha desplegado la diligencia necesaria al adaptar sus cláusulas informativas a lo señalado en cada caso por la Agencia, y que ha suprimido cualquier tipo de comunicación de datos personales recogidos en los ficheros de Ceac a entidades ajenas al Grupo Planeta, es preciso señalar que, cabe apreciar por ambas circunstancias, que concurre una cualificada disminución de la culpabilidad de Ceac por lo que procede aplicar el artículo 45.5 de la LOPD.
Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: ESTIMAR parcialmente el recurso de reposición interpuesto por **CENTRO DE ESTUDIOS CEAC, S.L.,** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 04/07/2006, en el procedimiento sancionador PS/00328/2005, e imponer una sanción de 60.101,21 € por la infracción del artículo 11 de la LOPD, a tenor de lo previsto en el artículo 44.4.b) en relación con el artículo 45.3, 4 y 5 de la citada Ley Orgánica.

SEGUNDO: **NOTIFICAR** la presente resolución a la entidad **CENTRO DE ESTUDIOS CEAC, S.L.,** (C/.....).

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.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, 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 del referido texto legal.

Audiencia Nacional. Sentencia de 8-02-2006. Sala Contenciosa-Administrativa, Sección Primera. Calidad de los Datos: Finalidad Incompatible.

La AN desestima el recurso. Madrid, a ocho de febrero de dos mil seis.

Vistos por la Sala citada al margen el Recurso número 01/495/2004 interpuesto por ENTIDAD A, representado por el procurador Sra . . . ., contra la resolución de fecha 27 de Julio de 2004 dictado por el Director de la Agencia Española de Protección de Datos por la que se sanciona a la entidad recurrente con una multa de 60.101,21 euros por infracción del artículo 4.2 de la ley orgánica 15/99 en relación con lo previsto en el artículo 44.3.d) de la misma ley, habiendo sido parte el Sr. Abogado del Estado. La cuantía del recurso ha sido fijada en 60.101,21 euros.

ANTECEDENTES DE HECHO.

PRIMERO: Por el indicado recurrente se interpuso recurso contencioso administrativo mediante escrito presentado ante esta sala contra el acto mencionado en el encabezamiento de esta resolución, acordándose su admisión y una vez formalizados los trámites legales preceptivos fue emplazado para que dedujera demanda, lo que llevó a efecto mediante escrito en el que, tras alegar los fundamentos de hecho y de derecho que consideró pertinentes, terminó solicitando la estimación del recurso y la consiguiente anulación del acto recurrido y solicitó que se deje sin efecto la sanción por no constituir el hecho imputado infracción del artículo 4.2 de la ley orgánica 15/99.
De lo que consta en el expediente .y de las alegaciones de las partes en sus respectivos escritos resulta el siguiente relato de hechos:
- . . . . . adquirió en diverso material docente en la empresa “ENTIDAD A” para preparar unas oposiciones quedando incluida en su fichero de clientes.
- . . . . . aprobó unas oposiciones de A TS/DUE y las listas de aprobados se publicaron en Internet en las páginas del Ministerio de Sanidad.
- Cuando “ENTIDAD A” comprobó que . . . . . había sido cliente suya y que aparecía como número 1 de la citada oposición, en la publicidad correspondiente al año 2003 incluyó una leyenda que decía "¡¡Excelentes resultados de nuestros alumnosii; 59 alumnos aprobados de “ENTIDAD A” y entre ellos los números N° 1 . . . . . .
- . . . . . , cuando conoció esta publicidad, se dirigió a la entidad recurrente manifestándole su oposición a que se utilizara su nombre por lo que se suprimió de la publicidad el nombre de la denunciante y se bloquearon sus datos del fichero de clientes.
- Por estos hechos . . . . . formuló denuncia con fecha 3 de Julio de 2003; tras la tramitación del correspondiente expediente sancionador se dictó la resolución que ahora es objeto del presente recurso contencioso administrativo.

SEGUNDO: La representación procesal de la parte demandada contestó a la demanda mediante escrito en el que, tras alegar los hechos y fundamentos de derecho que consideró aplicables, terminó pidiendo la desestimación del presente recurso.

TERCERO: Al no haberse recibido el pleito a prueba, se dio traslado a las partes, por su orden, para conclusiones; en este trámite se evacuó en sendos escritos en los que realizaron las manifestaciones que le convinieron a sus respectivos intereses.

CUARTO: Con fecha 7 de Febrero se celebró el acto de votación y fallo de este recurso, quedando el mismo visto para sentencia.
Ha sido ponente del presente recurso el Magistrado IItmo. Sr. . . . . .

FUNDAMENTOS JURÍDICOS

PRIMERO: Se interpone el presente recurso contencioso administrativo frente a la resolución de fecha 27 de Julio de 2004 dictada por el Director de la Agencia Española de Protección de Datos por la que sanciona a la entidad recurrente con una multa de 60.101,21 euros por infracción de-l artículo 4.2 de la ley orgánica 15/99 en relación con lo previsto en el artículo 44.3.d) de la misma ley.
La resolución recurrida considera que el uso dado por "ENTIDAD A" a los datos de la denunciante es un uso prohibido por el referido artículo 4.2 de la Ley Orgánica y ello pues no puede apreciarse compatibilidad de usos pues se trata de usos no previstos en la relación contractual con la empresa. Entiende que la utilización de los datos para esos usos hubiera exigido el consentimiento expreso de la interesada. .

SEGUNDO: El artículo 4 de la Ley orgánica 15/99 encabeza el Titulo correspondiente a los Principios de Protección de Datos y dicho artículo 4 se rubrica como "Calidad del dato" y su párrafo 2 dice que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".
A su vez, el artículo 44.3.d) sanciona como infracción grave "Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave".
La prohibición de utilizar datos para una finalidad incompatible o distinta de aquella para la que los mismos fueron recabados a que se refiere el artículo 4.2 es, pues, uno de los principios básicos de la protección de datos, en su título 11, de donde se desprende la importancia que en el sistema de la Ley reviste tal aplicación de datos a la finalidad para la que fueron pedidos.
Ello así resulta con claridad de relacionar el repetido artículo 4.2 de la LOPD con' el ordinal 1 del mismo artículo 4, que exige para que los datos puedan recogerse para su tratamiento que sean "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido", estableciéndose en definitiva en tal artículo 4 una sutil distinción entre finalidad de la recogida y finalidad del tratamiento pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines.
Así pues, y de acuerdo con el artículo 1.b) de la Directiva95/46/CE de 24 de octubre de 1995 (en cuya redacción se inspira tal artículo 4.2 de nuestra LOPO), si la recogida se hizo con fines determinados, cualquier uso o tratamiento posterior con finalidad distinta es incompatible con la primera finalidad que determinó su captura por lo que, en este contexto, diferente o incompatible significan lo mismo. (Así resulta de la sentencia de esta Sala dictada en el recurso 123/2003).
Evidentemente, cuando . . . . . adquirió determinado material a "ENTIDAD A" debe entenderse que consintió en la inclusión de sus datos en el fichero preciso para la remisión del material, la contabilidad, la gestión y el pago de dicho material; pero para lo que no consentía era para que sus datos fueran utilizados en la publicidad de la empresa ahora recurrente. . Claramente, pues, "ENTIDAD A", utilizó los datos de . . . . . para finalidad distinta de la que era previsible sin contar para ello con en consentimiento de la interesada, consentimiento cuya exigencia proviene de lo que señala el artículo 6 de la propia Ley Orgánica cuando dice que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

TERCERO: Esta Sala en la sentencia del recurso 119/2002' realizó una interpretación clara del artículo 4.2 de la Ley Orgánica 15/1999 en la que se dan respuesta a los argumentos de la entidad recurrente en relación a la interpretación del término "incompatibles" que emplea el artículo 4.2 de la Ley Orgánica 15/99.
Se dijo en aquella sentencia que *"aunque el artículo* 4;2 *de la Ley* 15/99, *en contraposición con el artículo* 4.2 *de la Ley* 5/92, ya *no* se *refiere* a *"finalidades distintas': sino* a *"finalidades incompatibles': revelando una ampliación de la posibilidad de utilización de los datos, sin embargo la interpretación sistemática del precepto* y *la ambigüedad del término '1inalidades incompatibles" avalan la interpretación realizada en el acto administrativo impugnado. En efecto, según el diccionario de la Real Academia "incompatibilidad" significa "repugnancia que tiene una cosa para unirse con otra,* o *de dos* o *más personas entre sí", por tanto, una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida* e *ilimitada de finalidades, pues es muy difícil imaginar usos que produzcan la repugnancia que evoca la incompatibilidad, por lo que "semejante interpretación conduce al absurdo* y *como tal ha de rechazarse", como hemos declarado en Sentencia de* 8 *de febrero de 2002. Teniendo en cuenta, además, que dicho término se introduce en el Ley de* 1999, *como ha declarado la doctrina, por una traducción poco precisa del artículo* 6 *de la Directiva* 46/1995, *de* 24 *de octubre.*
Conclusión igualmente avalada por la interpretación sistemática alud.ida, pues como señalamos en la citada Sentencia de 8 *de febrero de 2002, "semejante prescripción no puede ser entendida sino como un enunciado de carácter general, que no puede prevalecer sobre la regulación específica de una materia'" citando al efecto el artículo* 6 *de la citada Ley, y añadiendo que la interpretación de dicho artículo* 6.2, a *sensu contrario, impone "que cuando los datos* se *usen con otra finalidad distinta se precisará el consentimiento del afectado. Y no parece que el arto* 4.2, *venga* a *efectuar una ampliación sobre la posibilidad de utilización de los datos, como entiende el actor, porque ello supondría dejar sin contenido el arto* 6.2, *cuya redacción en este punto es igual* a su *homónimo de la Ley* 5/92".
El uso de los datos de la denunciante para la publicidad de la entidad recurrente es un uso que no solo es distinto sino que es un uso incompatible con el previsto cuando se recogieron los datos de la denunciante. Se trataba de una relación simplemente comercial respecto de la que no es posible admitir que "derive" hacía una relación que justifique la publicidad sobre la base de los resultados obtenidos por la denunciante que, por lo que parece, había preparado las oposiciones con otro centro aunque había comprado los libros en la entidad recurrente. Por todo lo dicho, parece suficientemente justificada la infracción del artículo 44.3.d) en relación con el artículo 4.2 de la Ley Orgánica 15/99 y justificado del mismo modo la imposición de la sanción.

CUARTO: La parte recurrente interesa, también, la aplicación de lo previsto en el artículo 45.5 de la Ley orgánica 15/99 que establece que "Si en razón de las circunstancias concurrentes se apreciara una cualificada disminución de la culpabilidad el imputado o de la antijuridicidad del hecho, 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".
Dicho precepto no es sino manifestación del llamado principio de proporcionalidad (art. 131.1 de la Ley 30/1992), incluido en el mas general de prohibición de exceso, y reconocido por la jurisprudencia como Principio General del Derecho. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y solo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancial mente atenuadas atendidas las circunstancias del caso concreto. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos.

La posibilidad prevista en el artículo 45.5 no es sino consecuencia del valor justicia que informa nuestro Ordenamiento Jurídico -arto 1 CE, en relación con las STC 50/1995 y 173/1995-. Siendo plasmación de tal principio que en casos de cualificada disminución de la culpa o de la antijuridicidad, sea posible disminuir en un grado la sanción aplicable. Ahora bien, la presente regla debe aplicarse con exquisita ponderación y solo en los casos en los que la culpabilidad y la antijuridicidad resulten sustancial mente atenuadas atendidas las circunstancias del caso concreto, de forma que repugne a la sensibilidad jurídica, siempre guiada por el valor justicia, la imposición de la sanción correspondiente al grado. Lo cual insistimos puede darse, por excepción, en casos muy extremos (de aquí la expresión "especialmente cualificada") y concretos.
La entidad recurrente considera que las razones que deben llevar en este caso a la aplicación de la reducción de la sanción que prevé dicho precepto son las siguientes:
- Que siempre ha manifestado un gran respeto por la protección de datos y tienen notificados y dados de alta en la Agencia sus ficheros de clientes.
- Que nunca ha tenido denuncias a pesar del alto número de clientes con los que cuenta.
- Que retiró el folleto de modo inmediato en cuanto conoció la queja de la denunciante y procedió a bloquear sus datos en sus ficheros.
- Que todo ha procedido de una interpretación errónea del precepto en cuestión y que dicha interpretación era disculpable en atención a la dicción del antiguo artículo 4.2 de la Ley de Protección de Datos.
- Que el folleto en el que se hizo un uso indebido de los datos de la denunciante eran unos folletos que no tenían carácter masificado y de un ámbito de tráfico limitado y con los que se pretendía acreditar la calidad de la enseñanza que se facilitaba y no inducir a engaño sobre ningún aspecto de su actividad.
También ha insistido la parte recurrente en que el dato de que la recurrente había sacado el número 1 en su oposición era un dato que aparecía en un medio de acceso general como era la página de Internet del Ministerio de Sanidad. No obstante, es necesario señalar que dicha fuente no tiene la consideración de fuente publica de acceso en el concepto que procede del artículo 3.D de la Ley Orgánica 15/99.
En cualquier caso resulta que no puede aplicarse el citado párrafo 5 del artículo 45 de la Ley Orgánica y ello pues no puede alegarse disminución de la culpabilidad en un caso como el presente en que ha habido un comportamiento malicioso desde el momento en que la empresa recurrente utiliza en su publicidad el nombre de la denunciante como si hubiera sido alumna suya cuando no era tal. sino que, simplemente, había comprado unos libros y se había preparado en otro Centro. Esta conducta, que permite hablar, en cierto modo, de publicidad falsa, es lo que impide, en este concreto supuesto, aplicar la disminución de culpabilidad con la consiguiente rebaja en la imposición de la sanción que pretendía la recurrente.

QUINTO: Por aplicación de lo establecido en el artículo 139 de la Ley de la Jurisdicción Contencioso Administrativa' no resulta procedente hacer expresa condena en costas a ninguna de las partes que han intervenido en este procedimiento.
Vistos los preceptos citados por las partes y los demás de general y pertinente aplicación al caso de autos .

FALLAMOS

Que desestimando el presente recurso contencioso administrativo interpuesto por el procurador . . . . . ., en la representación que ostenta de “ENTIDAD A”, contra la resolución descrita en el primer fundamento de esta Sentencia, debemos confirmar la

resolución recurrida. Todo ello sin haber lugar a expresa imposición de costas. Así por esta nuestra sentencia lo pronunciamos mandamos y fallamos.

PUBLICACIÓN. Dada, leída y publicada fue la anterior sentencia en audiencia pública.

Procedimiento Nº: TD/00168/2006

RESOLUCIÓN Nº.: R/00535/2006

Vista la reclamación formulada por **DON F.L.M.**, contra el **INSTITUTO DE ENSEÑANZA SECUNDARIA *"PABLO SERRANO*", DE ZARAGOZA**, y en base a los siguientes,

HECHOS

PRIMERO: Con fecha 17 de marzo de 2006, tuvo entrada en esta Agencia reclamación formulada por DON F.L.M. (en lo sucesivo el reclamante), por la denegación del derecho de oposición al tratamiento de sus datos contenidos en los ficheros del Instituto de Enseñanza Secundaria *"Pablo Serrano",* de Zaragoza (en lo sucesivo I.E.S.).

SEGUNDO: En fecha 18 de abril de 2006, se trasladó dicha reclamación al I.E.S., que presentó las alegaciones que a su derecho estimó convenientes, manifestando que cuando se recibió el ejercicio del derecho de oposición del reclamante se le contestó el mismo día, pidiéndole que informara sobre qué datos de carácter personal aparecen publicados en su página web que infringen la normativa de protección de datos. Lo que se publica son los horarios de los grupos de alumnos, los períodos de atención de los profesores tutores y los de atención que, como profesores de asignatura, área y/o módulo, aparecen en sus horarios personales para atender a las familias. Algunos de los datos personales que se utilizan han sido publicados en el Boletín Oficial del Estado, y el resto lo han sido considerando las obligaciones existentes para el Instituto en la normativa establecida por el Departamento de Educación y Ciencia que aprueba las Instrucciones que regulan la organización y funcionamiento de los Centros Públicos de Educación Secundaria de la Comunidad Autónoma. El artículo 6.4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), indica que deben existir motivos fundados y legítimos relativos a una concreta situación personal para oponerse al tratamiento de los datos.

TERCERO: Examinadas las alegaciones presentadas por el responsable del fichero, se dio traslado de las mismas al reclamante, que señaló que nadie del equipo directivo del I.E.S. se ha dirigido a él para informarse de los motivos que le llevan a oponerse al tratamiento de sus datos que se publican en la página web del mencionado Instituto.

CUARTO: Otorgada audiencia al responsable del fichero, éste se ratifica en las manifestaciones realizadas con anterioridad.

HECHOS PROBADOS

PRIMERO: Con fecha 25 de enero de 2006, Don F.L.M. se dirigió al I.E.S. solicitando lo siguiente: "*En la página web del Centro aparecen publicados datos de carácter estrictamente personal... Que en el plazo que la LOPD establece, el responsable del fichero excluya del tratamiento los datos relativos a mi persona, que no sean fuentes de acceso público. Quede clara mi oposición al tratamiento de dichos datos."*

SEGUNDO: En fecha 25 de enero de 2006, el I.E.S. contestó a Don F.L.M. en el sentido siguiente: *"Le solicito nos indique los datos de carácter estrictamente personal que aparecen publicados en nuestra página web y el artículo de la LOPD en el que se reconoce ese, supuesto, derecho que el Instituto está infringiendo".*

FUNDAMENTOS DE DERECHO

PRIMERO: La competencia para resolver la presente reclamación corresponde al Director de la Agencia Española de Protección de Datos, de acuerdo con el artículo 37.d) en relación con el artículo 36 de la LOPD.

SEGUNDO: El artículo 18.1 de la LOPD señala que "*Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine*".

TERCERO: Respecto al citado derecho de oposición, el artículo 17 de la LOPD señala lo siguiente: *"Los procedimientos para ejercitar el derecho de oposición, acceso así como los de rectificación y cancelación serán establecidos reglamentariamente."*
La vigente LOPD incorpora, trasponiendo la Directiva 95/46/CE, el derecho de oposición, junto a los derechos de acceso, rectificación y cancelación ya previstos en la derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.
La cuestión que se plantea, por tanto, atendiendo al tenor de la LOPD respecto al derecho de oposición y a la normativa preexistente declarada en vigor por la disposición transitoria tercera de la LOPD es la de si, interpretadas sistemáticamente, cabe concluir que el ejercicio del derecho de oposición puede integrarse en el desarrollo reglamentario que la Ley Orgánica declara subsistente. En este sentido se plantean, al menos, tres cuestiones básicas.
En primer lugar, la relativa a la naturaleza de dicho derecho y a las condiciones para su ejercicio. A este respecto no cabe duda de que estamos en presencia de un derecho personalísimo (art. 11 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que se encuentra vigente de conformidad con lo que dispone la disposición transitoria tercera de la LOPD) que se ejercerá independientemente de los restantes derechos reconocidos en la LOPD por su titular – excepto en los supuestos limitados en los que cabe la representación –, el cual deberá acreditar su identidad (art. 11 y Norma Primera de la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación), sin que quepa exigir contraprestación alguna por su ejercicio).
En segundo lugar, la que afecta a los plazos para resolver sobre la petición de oposición al tratamiento de datos y a la necesidad de contestar a las solicitudes a través de las cuales se ejerza este derecho. En este sentido, cabe reseñar que el artículo 17 de la LOPD, que remite al desarrollo reglamentario el ejercicio de los derechos, distingue entre los relacionados con los derechos de acceso y oposición y los de rectificación y cancelación como se desprende de la expresión *" ..así como..."* que viene a diferenciar dos bloques distintos entre unos y otros, excepto en lo que sean de aplicación las normas comunes a todos ellos. En esta línea, el plazo para atender el derecho de oposición deberá ser el de un mes, que coincide con el previsto para el derecho de acceso y se diferencia del plazo para hacer efectivo los derechos de rectificación y cancelación.
Ha de señalarse que una interpretación contraria no sería conforme con la Directiva 95/46/CE, por cuanto que implicaría la inexistencia de un plazo para el ejercicio del nuevo derecho de oposición que la norma comunitaria obliga a incorporar y proteger en el derecho interno, con la consecuencia de que la LOPD no habría transpuesto dicha Directiva al no contemplar plazo para su satisfacción, quedando impune la falta de respuesta frente a su ejercicio. Y, no debe olvidarse a este respecto, que la

voluntad expresa del Legislador al aprobar una nueva LOPD y derogar la citada Ley Orgánica 5/1992, fue la de trasponer totalmente aquella Directiva.
De ahí que, tanto la obligación asumida por el Legislador de incorporar a nuestro derecho interno la Directiva Comunitaria, como una interpretación en pro del contenido esencial del derecho fundamental a la protección de datos (Sentencias del Tribunal Constitucional 290 y 292/2000, de 30 de noviembre) permiten interpretar la literalidad del artículo 17 en los términos expuestos.
Quedarán a salvo, lógicamente, los desarrollos reglamentarios del derecho de acceso que resultan incompatibles con el contenido propio del derecho de oposición, pero no los relativos al plazo en que debe ser atendido.
En tercer lugar, ha de atenderse a los aspectos procedimentales relativos a la posibilidad de ser objeto de reclamación ante la Agencia (artículo 18 LOPD) y a la tramitación de las reclamaciones que se planteen. En este punto no cabe duda de que el mencionado artículo 18 de la LOPD establece una regla general relativa a la tutela de todos los derechos, consistente en que cualquier actuación contraria podrá ser objeto de reclamación ante la Agencia (apartado 1), y que, aquél al que se deniegue total o parcialmente su ejercicio podrá ponerlo en conocimiento de ésta con la obligación, por parte de la autoridad de control, de asegurarse de la procedencia o improcedencia de la denegación, dictando resolución en el plazo máximo de seis meses (apartado 2).
Y, tampoco cabe duda de que serán aplicables las disposiciones generales relativas a la tutela de derechos – en particular el artículo 17 del citado Real Decreto 1332/1994 - y los requisitos generales que para su ejercicio contempla la Norma Primera, punto 4, de la mencionada Instrucción 1/1988, cuando dispone lo siguiente: *"4. El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.*
En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos".

QUINTO: El artículo 14.b) de la Directiva 95/46/CE establece que: *"Los estados miembros reconocerán el interesado el derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección..."*
El artículo 6.4 de la LOPD establece una previsión específica respecto del derecho de oposición, según el cual *"En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una situación concreta. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado"* (el subrayado es de la Agencia Española de Protección de Datos).

SEXTO: En el supuesto presente, ha quedado acreditado que el reclamante ejerció el derecho de oposición al tratamiento de sus datos personales por parte del I.E.S., con la finalidad de que no se publicasen en la página web del citado Instituto. El I.E.S. contestó, el mismo día que recibió la solicitud de oposición, solicitando al reclamante que indicase los datos de carácter estrictamente personal que aparecen publicados en la página web y el artículo de la LOPD en el que se reconoce el derecho que el Instituto está infringiendo. Sin embargo, como se indica en los Fundamentos de Derecho anteriores, el I.E.S. no procedió a subsanar la solicitud en el sentido de que el reclamante especificara cuáles eran los motivos fundados y legítimos relativos a su situación concreta en los que basaba su derecho de oposición, tal y como exige el

artículo 6.4 de la LOPD. Por tanto, procede estimar la presente reclamación de tutela de derechos.
Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**
PRIMERO: ESTIMAR la reclamación formulada por **DON F.L.M.** e instar al **INSTITUTO DE ENSEÑANZA SECUNDARIA *"PABLO SERRANO*", DE ZARAGOZA** para que, subsane la solicitud presentada por éste y remita, en el plazo de los diez días hábiles siguientes a la notificación de la presente resolución, al reclamante certificación en la que se conteste motivadamente al derecho de oposición ejercitado, o motive las causas que lo impiden, pudiendo incurrir en su defecto en una de las infracciones previstas en el artículo 44 de la LOPD. Las actuaciones realizadas como consecuencia de la presente resolución deberán ser comunicadas a esta Agencia en idéntico plazo.

SEGUNDO: NOTIFICAR la presente resolución al **INSTITUTO DE ENSEÑANZA SECUNDARIA *"PABLO SERRANO*", DE ZARAGOZA,** (C/.....), y a **DON F.L.M.**, (C/.....).
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.
Contra esta resolución, que pone fin a la vía administrativa (artículo 18.4 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa (en 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.

Procedimiento Nº: TD/00531/2006

RESOLUCIÓN Nº.: R/00196/2007
Vista la reclamación formulada por **Dña. Y.M.M.**, contra la **ASOCIACIÓN DE CENTROS DE ENSEÑANZA PRIVADA DE ALBACETE**, y en base a los siguientes,
HECHOS

PRIMERO: Con fecha 27/10/06, tuvo entrada en esta Agencia reclamación formulada por Dña. Y.M.M. (en lo sucesivo la reclamante), por la denegación del derecho de acceso a sus datos contenidos en los ficheros de la Asociación de Centros de Enseñanza Privada de Albacete (en lo sucesivo, ACEPA).

SEGUNDO: En fecha 22/11/06, se trasladó dicha reclamación a ACEPA, que presentó las alegaciones que a su derecho estimó convenientes manifestando que no se atendió la solicitud de acceso de la reclamante pues no iba acompañada de fotocopia de su documento nacional de identidad para garantizar su identificación como titular de los datos sobre los cuales se ejercita el citado derecho de acceso. Manifiesta asimismo los datos de la reclamante le fueron facilitados por un particular y ACEPA los utilizó para enviarle una carta en relación con su actividad consistente en impartir clases particulares, actividad que no se encontraba regularizada. Finalmente señala los datos de la reclamante no figuran registrados ni almacenados en archivo alguno.

TERCERO: Examinadas las alegaciones presentadas por el responsable del fichero, se dio traslado de las mismas al reclamante, que señaló no efectuó alegación alguna.

HECHOS PROBADOS

PRIMERO: Con fecha 05/05/06, Dña. Y.M.M. solicitó por correo certificado el acceso a sus datos personales contenidos en los ficheros de ACEPA sin que ésta respondiera dicha solicitud.

SEGUNDO: Con fecha 27/10/06, Dña. Y.M.M. presentó reclamación de Tutela de Derechos por la denegación del derecho de acceso a sus datos en los ficheros de ACEPA.

FUNDAMENTOS DE DERECHO

PRIMERO: La competencia para resolver la presente reclamación corresponde al Director de la Agencia Española de Protección de Datos, de acuerdo con 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).

SEGUNDO: El artículo 18.1 de la LOPD señala que "*Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine*".

TERCERO: El artículo 15.1 de la LOPD dispone que "*El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos"*.

CUARTO: El artículo 12.1, 3 y 4 del Real Decreto 1332/94, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, que continúa en vigor de conformidad con lo establecido en la disposición transitoria tercera de la LOPD, determina:
"*1. El derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar*".
"*3. El responsable del fichero resolverá sobre la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992*," (artículo 18.1 LOPD).
"4. Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla" (el subrayado es de la Agencia Española de Protección de Datos).
En cuanto al contenido de la información, el artículo 13, apartado 2 del mismo Real Decreto señala: "*La información comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos".*

QUINTO: Por su parte, la Instrucción 1/1998, de 19 de enero, de la Agencia Española de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación establece en los puntos 3 y 4 de su Norma Primera lo siguiente:
"3. *El ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:*
Nombre, apellidos del interesado y fotocopia del documento nacional de identidad del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.
Petición en que se concreta la solicitud.
Domicilio a efectos de notificaciones, fecha y firma del solicitante.
Documentos acreditativos de la petición que formula, en su caso.
El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción."
"4. El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.
En el caso de que la solicitud no reúna los requisitos especificados en el apartado tercero, el responsable del fichero deberá solicitar la subsanación de los mismos" (el subrayado es de la Agencia Española de Protección de Datos).

SEXTO: En el presente caso,ha quedado acreditado que el 05/05/06, la reclamante se dirigió a ACEPA. solicitando el acceso a su datos, sin que haya obtenido, como era su obligación a tenor de la normativa citada, contestación alguna por parte de la entidad, motivo por el cual procede la estimación del presente procedimiento de Tutela de Derechos.
Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: ESTIMAR la reclamación formulada por **DÑA. Y.M.M.** e instar a la **ASOCIACIÓN DE CENTROS DE ENSEÑANZA PRIVADA DE ALBACETE**, para que, en el plazo de los diez días hábiles siguientes a la notificación de la presente resolución, remita al

4/4

reclamante certificación en la que se haga constar los datos personales existentes en sus ficheros, o motive las causas que lo impiden, pudiendo incurrir en su defecto en una de las infracciones previstas en el artículo 44 de la LOPD. Las actuaciones realizadas como consecuencia de la presente resolución deberán ser comunicadas a esta Agencia en idéntico plazo.

SEGUNDO: NOTIFICAR la presente resolución a la **ASOCIACIÓN DE CENTROS DE ENSEÑANZA PRIVADA DE ALBACETE**, y a **DÑA. Y.M.M.**, (C/.....….....).

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.

Contra esta resolución, que pone fin a la vía administrativa (artículo 18.4 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa (en 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.