Informe 0477/2009

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 articulo 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.