

La vuelta al cole y la protección de datos. La exposición de los menores en Internet.

Lucía Miralles

El verano ha llegado a su fin y con él la esperada vuelta al cole. Sin embargo, estas semanas no sólo deben significar la compra de libros, mochilas o uniformes, sino que podríamos aprovechar para reflexionar sobre la importancia de la educación digital y el papel esencial de los centros educativos en el cumplimiento de la normativa de protección de datos. Las nuevas tecnologías forman parte de nuestra vida cotidiana y la exposición de los menores es cada vez más habitual, sin tener en cuenta los peligros que ello conlleva.

En muchas ocasiones la protección de datos suena a trámite, a esa casilla que hay que marcar para realizar casi cualquier gestión, desde inscribirse en un boletín, reservar mesa en un restaurante o hacer una compra online. Pero la protección de datos personales cobra especial relevancia cuando los sujetos del tratamiento son menores de edad.

Los niños son sujetos vulnerables, por lo que sus datos personales deben estar especialmente protegidos por sus madres/padres, tutores o representantes legales, aunque no siempre depende de estos la observancia que conlleva el tratamiento de los datos personales. Cuando los pequeños se encuentran en el colegio, las personas encargadas de velar por la protección de sus datos son los docentes y el personal que forma parte del centro.

La vuelta al cole puede parecer que lleva consigo únicamente la compra de material escolar y uniformes, pero no debe desaprovecharse la oportunidad de parar por un momento y reflexionar sobre la importancia de proteger los datos personales de los menores en los centros educativos y así desarrollar conductas que velen por los derechos de los pequeños. Esta reflexión, desde los colegios, puede materializarse en dos áreas: por un lado, la educación digital, entendiendo con ello el uso que hacen los niños de los dispositivos electrónicos e internet, y, por otro, la diligencia de los centros en el cumplimiento de la normativa de protección de datos.

La tecnología evoluciona a la velocidad de la luz y las nuevas generaciones son las primeras en adaptarse y

Agencia Española de Protección de Datos (AEPD) señalan en su web "más que un móvil" que "el 94,8% de los adolescentes dispone de móvil con conexión a Internet, dispositivo al que acceden antes de los 11 años por término medio. El 92,2% de los estudiantes de 1.º y 2.º de ESO tienen smartphone propio". Estas cifras son a la vez sorprendentes y preocupantes.

La educación digital es imprescindible para que los menores sean conscientes de los peligros que conlleva disponer de un dispositivo móvil con acceso a internet. El ciberacoso, el envío de fotografías comprometidas o la relación con adultos desconocidos son algunos de los peligros más comunes que se señalan desde la AEPD. Asimismo, el *grooming*[1], la pornografía infantil o el *sexting*[2] son otras de las modalidades que pueden llegar a producirse.

La tecnología evoluciona a la velocidad de la luz y las nuevas generaciones son las primeras en adaptarse y adoptarla.

La responsabilidad de educar sobre las implicaciones de las novedades en el sector digital no atañe únicamente a los padres, tutores o representantes legales de los menores, sino también a los centros educativos o colegios. En estos últimos, la figura del "coordinador de bienestar y protección" es esencial y surge de la necesidad imperiosa de prevenir abusos, detectar posibles conflictos en una fase temprana, proporcionar un espacio seguro donde los menores puedan comunicarse y decidir dónde acudir si se ven envueltos en algún tipo de incidente que les afecte. Este coordinador es de obligada implantación desde la entrada en vigor de la Ley Orgánica 8/2021 de protección integral de la infancia y la adolescencia contra la violencia.

Por otra parte, los centros educativos tratan inevitablemente los datos personales de los alumnos

debiendo ser sumamente diligentes dada la especial protección que requieren. Archivos fotográficos y audiovisuales, autorizaciones, expedientes disciplinarios, intervención en la gestión de ayudas, becas y subvenciones, traslados de expedientes o videovigilancia son algunos de los tratamientos habituales que tienen lugar en ellos. Por ello, la AEPD ha querido señalar los casos más comunes sobre los que se han planteado reclamaciones como son la publicación de las listas de alumnado admitido o de las calificaciones escolares, la grabación de los menores o la captación de fotografías de los mismos, entre otros.

La educación digital es imprescindible para que los menores sean conscientes de los peligros que conlleva disponer de un dispositivo móvil con acceso a internet.

Uno de los puntos más controvertidos en la actualidad, y que más denuncias ha suscitado ante la AEPD, es la sobreexposición y publicación de imágenes de menores por parte de colegios y centros educativos, sin el consentimiento de sus padres, tutores o representantes legales. Cada imagen que identifique a un niño o niña ya no solo debe ir acompañada del consentimiento de sus padres, madres o tutores legales en caso de ser menores de 14 años (edad fijada en España por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales), sino que debe ir de la mano de una ponderación y valoración del centro escolar que desde la sensatez decida publicar dicha fotografía.

La publicación de fotografías de menores es un tratamiento de datos personales que requiere de una base de legitimación. En este caso, la base de legiti-

[1] Entendido en palabras de *Save the Children* como: "El grooming y, en su evolución digital, el online grooming (acoso y abuso sexual online) son formas delictivas de acoso que implican a un adulto que se pone en contacto con un niño, niña o adolescente con el fin de ganarse poco a poco su confianza para luego involucrarle en una actividad sexual".

[2] Según el INCIBE: "El Sexting es una práctica de riesgo que consiste en el envío de fotografías o vídeos producidos por uno mismo con connotación sexual a través del teléfono móvil u otro dispositivo con conexión a Internet".

mación legitimación es el consentimiento, por lo que los centros escolares deberán recabarlo de forma correcta comprobando la edad del menor así como si el mismo reúne los requisitos necesarios de validez (acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal), tanto si se ofrece personalmente como si corresponde a padres, tutores o representantes legales.

Recientemente, la AEPD ha sancionado a un colegio con 15.000€, sin bien finalmente el centro educativo pagó 9.000€ acogiéndose a los descuentos por pronto pago, por la publicación de imágenes de un menor en la cuenta de Facebook del centro y en una lista de difusión de WhatsApp no solo sin mediar el consentimiento de sus padres, sino habiéndose opuesto expresamente a dicha circunstancia. Esta es una conducta común que no contempla los peligros que puede suponer la difusión de las imágenes de los niños.

Cada imagen que identifique a un niño o niña ya no solo debe ir acompañada del consentimiento de sus padres, madres o tutores legales en caso de ser menores de 14 años (...), sino que debe ir de la mano de una ponderación y valoración del centro escolar que desde la sensatez decida publicar dicha fotografía.

En muchos casos no somos conscientes de que, si las imágenes son públicas, cualquiera puede tener acceso a las mismas y los riesgos que pueden entrañar aumentan exponencialmente. Por ello, a pesar de recabar el consentimiento válidamente desde los centros ha de realizarse un juicio crítico sobre la necesidad y procedencia de la publicación de determinadas fotografías.

En definitiva, **la exposición de los menores en Internet no es inevitable** y debe estar controlada y supervisada por los sujetos responsables, en este caso, los centros escolares, y autorizada por los padres, tutores o representantes legales.