

Que no te hagan famoso

Rubén Lahiguera
Asociado de Privacidad
y Protección de Datos



EXPANSIÓN
2016, 2017,
2018 y 2019

**Premio Expansión al
proyecto más innovador**



FINANCIAL
TIMES
2018

**Seleccionada por
Financial Times entre
las 50 Firmas más
innovadoras de
Europa**

THE LAWYER
2019

**Premio The Lawyer a la
mejor Firma en TMT de
Europa**



**Seleccionada en Banda
1 por Chambers and
Partners y Legal 500
en TMT**



FORBES
2017

**Premio Forbes a la mejor
Firma de tecnología de
España**

ECIJA

Un análisis sobre la utilización de la imagen de los menores en internet y las diferentes consecuencias derivadas de las condiciones de su utilización en centros educativos.

Me he permitido transformar el antiguo hashtag **#NoSeasFamoso**, perteneciente a una campaña de UNICEF para la protección de los menores en internet, con el fin de introducir en este artículo un análisis sobre la utilización de la imagen de este colectivo en entornos tecnológicos, especialmente durante su estancia en centros educativos.

Hace pocas semanas se anunció la colaboración entre la Agencia española de protección de datos y la Fundación ProFuturo con el fin de impulsar iniciativas de responsabilidad social en el marco de la educación y los menores lo que, unido a la reciente puesta a disposición de los ciudadanos de una plataforma en la que poder solicitar la retirada de Internet de videos e imágenes de ciberacoso o sexting, conforman una sólida base para asistir y formar a los menores de edad en esta materia, pues su exposición ante las redes sociales y nuevas tecnologías es mayor, y, al mismo tiempo, su percepción de los riesgos y consecuencias es, a menudo, mínima o inexistente.

Como concepto introductorio, la imagen de una persona constituye un elemento característico de su esfera personal y, como tal, se encuentra

dentro del ámbito de control de aquella. Además, resulta un instrumento clave de identificación y distinción del resto de individuos y, en consecuencia, se muestra idóneo para multitud de **situaciones cotidianas**.

Así, por ejemplo, mediante el uso de la imagen de una persona, es posible comprobar el cumplimiento por parte de un sujeto de obligaciones determinadas (acudir a un puesto de trabajo, encontrarse en un lugar determinado, realizar o abstenerse de realizar ciertas acciones); explotar los rasgos físicos personales de un sujeto atribuyéndolos a la comercialización de un bien o servicio, o difundir información relativa a la esfera privada (o pública, si se quiere) de un sujeto, ya sea a través de medios analógicos o digitales.

En el caso de los **centros educativos**, los usos habituales de la imagen de los alumnos se circunscriben, normalmente, a su identificación como medio de control, supervisión y protección durante su estancia en aquellos, a controlar su asistencia a clase o a otras actividades y, por último, a divulgarla con ocasión de actividades educativas o lúdicas (fiestas de graduación, concursos, eventos deportivos, etc.), mediando el preceptivo consentimiento.



Frente a los métodos tradicionales, últimamente se han venido planteando **usos innovadores** de la imagen de los alumnos en centros educativos para alcanzar alguno de estos fines, pero, en estos casos, atendiendo a la vertiente de la imagen que permite la identificación unívoca de una persona utilizando medios técnicos específicos; me estoy refiriendo a recurrir a técnicas de reconocimiento facial para, por ejemplo, detectar la presencia de un alumno en un lugar específico o para acceder a este. En estas circunstancias, la imagen del menor tiene la consideración de **dato biométrico** y, desde este punto de vista, este tratamiento debe someterse a las exigencias legales respecto a las denominadas categorías especiales de datos, como puede ser su tratamiento, excepcionalmente, en casos tasados (artículo 9 del RGPD) y, en su caso, a la realización de la correspondiente evaluación de impacto.

Respecto a los fines promocionales o de difusión de los centros educativos, es frecuente que puedan surgir problemas de diversa índole derivados de, por ejemplo, la concurrencia del consentimiento de ambos progenitores, cuando ambos ostenten la patria potestad para dicho uso (teniendo en cuenta que los mayores de 14 años pueden prestar el consentimiento por sí mismos); los fines específicos del uso de la imagen en cuestión, considerando el carácter restrictivo del derecho de imagen o el tratamiento de la imagen de menores por terceros ajenos al centro educativo, con fines privados o domésticos en el marco de eventos de gran afluencia.

Pero, además, no hay que olvidar que la imagen de los alumnos puede ser captada y utilizada también por sus propios compañeros y, precisamente, el fácil acceso de este colectivo a dispositivos móviles con cámara ha propiciado en los últimos años usos fraudulentos de la imagen de terceros.

Estos comportamientos se caracterizan, principalmente, por no ser consentidos por el propio afectado (o, por lo menos, no, para diferentes usos posteriores) y por que el uso no autorizado de la imagen suele consistir en su divulgación al público. Algunos de ellos son:

Ciberacoso o cyberbullying

Supone la utilización de medios digitales y, más habitualmente, de redes sociales, con el fin de acosar a un sujeto. Este acoso puede llevarse a cabo a través de la divulgación de información, ya sea real o falsa, sobre una persona, y, frecuentemente, sobre la imagen de esta, de forma que se menoscaba su personalidad y se lesiona su integridad moral y su libertad. Esta conducta puede ser constitutiva de un delito tipificado con una pena de prisión de tres meses a dos años.

Sexteo o sexting

Es cada vez más frecuente que los jóvenes se inicien a una edad temprana en actividades que impliquen la utilización de medios digitales consistentes en la transmisión de imágenes propias o de terceros con fines eróticos o sexuales. Sin embargo, estas prácticas (en ocasiones consentidas y enmarcadas en una relación sentimental) pueden derivar en otras conductas que suponen un tratamiento ilícito de datos personales, como consecuencia de su deliberado reenvío a tercero sin consentimiento del afectado, o divulgación al público, a través de las redes sociales u otros medios de mensajería instantánea.

Suplantación de identidad

Esta conducta puede ser instrumental para realizar cualquiera de las mencionadas anteriormente, cuando se emplea una identidad falsa para hacer creer a los demás que el afectado está realizando las conductas en cuestión y, por lo tanto, que consiente dichas actividades.

Con independencia de las consecuencias jurídicas derivadas de estas conductas para los menores de edad, cabe destacar otras de carácter físico o psicológico como pérdida de peso, depresión, desórdenes como la anorexia o la bulimia, adicción a redes sociales o incluso ideas suicidas.

Los centros educativos, en estos casos, cuentan con una legitimación especial derivada del interés público para acceder al contenido de un dispositivo electrónico sin consentimiento, con el fin de atajar estas prácticas, siempre atendiendo al caso concreto y a los intereses en juego y, de conformidad con su protocolo interno.

Sin embargo, es habitual la ausencia de políticas de uso de dispositivos móviles en los centros escolares, así como de canales internos de denuncia de este tipo de conductas, lo cual está propiciado, seguramente, por la falta de formación del sector y el desconocimiento de la legislación sobre protección de datos que les resulta de aplicación.

Por todo ello, la concienciación y la formación son elementos esenciales para abordar estos problemas, máxime teniendo en cuenta que, tanto el RGPD como la propia Ley Orgánica de protección de datos y garantía de los derechos digitales (LOPDGDD) establecen expresamente el derecho a una educación digital que garantice el uso serio y respetuoso por parte del alumnado de los medios digitales (artículo 83 LOPDGDD). Por su parte, también la Ley Orgánica de Educación establece, como uno de sus principales fines, una formación óptima para asegurar la inserción del alumnado en la sociedad digital y el aprendizaje en el uso de medios digitales.

En definitiva, el establecimiento de políticas internas y canales específicos para la denuncia de conductas de cyberbullying u otras, una formación, tanto a profesores como a alumnos, sobre el uso responsable de este tipo de tecnología y,

finalmente, información clara y sencilla sobre los derechos que les amparan en materia de protección de datos e imagen resultan de vital importancia para cambiar esta tendencia.

Rubén Lahiguera

Asociado de Privacidad y Protección de Datos





Área de Privacidad y Protección de Datos de ECIJA
info@ecija.com | +34 91. 781.61.60