# Tipologías, gestión y prevención del cyberbullying en la escuela

Beatriz Sainz-de-Abajo[1], Luis Ojeda Martínez[2]

[1]*Profesora e Investigadora en el Departamento de Teoría de la Señal y Comunicaciones e Ingeniería Telemática*
*Universidad de Valladolid*
*España*
*E-mail: beatriz.sainz@tel.uva.es*

[2]*Inspector de Policía Local del Excmo. Ayuntamiento de Jaén*
*España*
*E-mail: lojema@andaluciajunta.es*

**Resumen**
Las nuevas generaciones se manejan con soltura en las redes sociales, lo que es un peligro por los depredadores sexuales y por la violencia a que pueden verse expuestos nuestros niños. Por eso es necesario que educadores, y familia, tengamos la información y formación suficiente para saber orientar en un uso responsable de las TIC. Hemos de conocer sus riesgos y sobre todo aprender a evitarlos, para así poder orientar a niños y jóvenes, muy vulnerables ante los mismos, haciendo de la prevención nuestra máxima aliada. El objetivo que persigue este documento es el análisis de fenómenos relacionados con el ciberacoso, que incluye términos como *cyberbullying, cyberstalking, sexting, cyberbaiting* y *grooming*, entendiendo los factores asociados a estas conductas, y proponer soluciones eficaces para su erradicación activando los mecanismos adecuados.

**Palabras clave:** *cyberbullying; cyberstalking; sexting; cyberbaiting; grooming*; menores; redes sociales; prevención.

## 1. Introducción.

El Instituto Nacional de Estadística (INE) de España difundió en noviembre de 2019, en su informe anual, que el uso de las Tecnologías de la Información y las Comunicaciones (TIC) está cada vez más extendido entre los menores de 10 y 15 años. En cifras cuantitativas el 66% dispone de teléfono móvil, un 89,7% posee ordenador y el 92,9% hace uso frecuente de Internet (Consejo General de la Psicología de España, 2019).

No hay que desdeñar las ventajas que ofrece Internet, que ha transformado en los últimos años la manera de acceder al visionado de los contenidos, junto con el ocio ilimitado que ofrecen las plataformas.

Las TIC han permitido nuevos espacios de socialización. Las nuevas generaciones han interiorizado el entorno virtual como algo necesario para socializar. Los nativos digitales han crecido inmersos en el mundo digital y todo lo que les ofrece la tecnología no les es ajeno (Prensky, 2014). Los inmigrantes digitales, por el contrario, se han visto abocados a aprender el uso de estas TIC, para no quedar atrás en este nuevo tipo de comunicación que, a veces, resulta autoimpuesto. Es en este nuevo paradigma de comunicación e interacción digital en el que los jóvenes deben desarrollar estrategias que les permitan, de modo correcto, gestionar sus relaciones de forma sana y ética.

No es infrecuente ver cómo los jóvenes se citan en lugares físicos para interaccionar a través de sus dispositivos móviles. Se comunican, aunque de diferente manera a como lo hacían generaciones anteriores. Ni se miran ni se hablan. Están absortos en sus pantallas, posiblemente intercambiando imágenes, vídeos o mensajes. Es un nuevo contexto en el que la forma tradicional de comunicación ha mutado. Acceden a prácticamente cualquier información, juegan online, experimentan con las redes sociales, generan sus perfiles y los actualizan, o lo hacen sus padres por ellos si no tienen edad mínima.

Da igual la hora, el lugar y momento del día o lo que esté ocurriendo, parece que siempre estemos disponibles para atender nuestras redes sociales. Nos comunicamos atemporalmente con nuestros conocidos, o los nuevos amigos, algunos de los cuales no conocemos personalmente. A pesar de que son herramientas desarrolladas en la mayoría de los casos para una comunicación asíncrona, hay un deseo que nos impulsa a consultar reiteradamente el dispositivo cada vez que oímos la entrada de un mensaje, o el comentario a un post que hayamos colgado en nuestro muro de la red social. Es un medio genial para difundir nuestro mensaje y facilitar la comunicación. También es un altavoz de nuestros pensamientos, ideas, imágenes, pero con un peligro cierto de que todo lo que se suba a Internet quedará en la Red para siempre, pudiendo caer en manos de quien no debiera aquello que se ha compartido.

Es casi una imposición formar parte de determinadas redes sociales para no quedar al margen de tu círculo de amistades. Si no estás en determinados grupos de aplicaciones para chatear, como WhatsApp, Telegram, Face time, Viber, Line, Skype, algunas de las más conocidas, no te enteras de las citas offline. La persona que no quiera quedarse excluida no tiene opción: o instala la aplicación subscribiéndose al grupo y está dentro o no se enterará de las novedades.

Sin embargo, a la multitud de ventajas debemos sumar los peligros reales e inherentes de las tecnologías. Escudados en el anonimato que ofrecen las redes, algunos desaprensivos, valiéndose de calumnias, *fake news*, fotos reales o retocadas, etc., destruyen la reputación de los demás. El hecho de no conocer la reacción que

provoca en la persona afectada los vuelve más osados y procaces en los comentarios, porque no se empatiza con el sujeto al que estamos atacando.

Inocentemente creemos que nuestra forma de actuar en el mundo virtual no tiene reflejo en el real. Y eso nos hace asumir riesgos que traen graves consecuencias. Porque nadie en su sano juicio se pasearía en ropa interior por la calle y, sin embargo, incomprensiblemente somos capaces de mandarle a un desconocido fotos semidesnudos. ¡Eso es ser muy osado y temerario!

En docencia las tecnologías han permitido la creación de espacios educativos virtuales, basados en modelos pedagógicos que posibilitan el aprendizaje mediante estrategias innovadoras (Díaz et al., 2011). Los profesores facilitan los contenidos a sus alumnos, disponibles en plataformas virtuales a través de dispositivos digitales. En Internet contamos con información ilimitada, 24 horas al día los 365 días del año, que crece de forma exponencial, aunque no siempre sea toda ella veraz. Debemos ser muy críticos con lo que leemos, contrastar y tratar de consultar los datos de fuentes fiables.

Las TIC han permitido una interacción fluida, síncrona y colaborativa para el intercambio de ideas y discusión que puede ser muy fértil para el desarrollo científico. En el escenario de aislamiento que hemos vivido, como consecuencia de la pandemia del Covid-19, hemos podido continuar la labor docente gracias a la multitud de herramientas disponibles para un seguimiento y gestión de la evaluación de los discentes, algo que hace pocos años no hubiera sido posible. Estas herramientas han hecho factibles los foros de discusión, las videoconferencias con multitud de actores y la grabación de contenidos de calidad para su difusión. En definitiva, nos ha permitido una continuidad de la docencia.

En el aula, la violencia y el acoso a los escolares no es una novedad. No obstante las TIC ofrecen un nuevo contexto donde ejercer violencia (Miró Llinares, 2013). Conocer estas formas de acoso, las consecuencias psicológicas en las víctimas, así como las herramientas para su prevención y gestión, una vez el problema ha tenido lugar, permitiría una asistencia más ajustada y eficaz. Por tanto, desde las instituciones es primordial dotar de profesionales que conozcan estas estrategias de prevención. Debemos recordar que en una sola generación hemos pasado de padres y educadores, casi analfabetos digitales, a hijos que navegan por las procelosas aguas de la tecnología digital con gran soltura, siendo Internet un espacio cotidiano para sus relaciones interpersonales.

Los padres, para salvaguardar la intimidad de sus hijos, tienden a ser restrictivos en el uso de las redes sociales. Con ello conseguimos el efecto contrario. Para evitar la prohibición al acceso a Internet, el menor no verbaliza sus problemas en la Red. El ser nativo digital les hace creer que son capaces de solucionar un problema por el hecho de conocer bien las nuevas tecnologías, pero son mentalmente inmaduros para afrontar determinadas situaciones.

## 2. Objetivo del trabajo.

Este documento describe las tipologías del ciberacoso al menor que incluye términos como *cyberbullying, cyberstalking, sexting, fake news* y *grooming*. Tras el análisis se hace una propuesta de recomendaciones eficaces para prevenir o minimizar los efectos en caso de que estos se produzcan.

## 3. Tipos de ciberacoso entre menores.

La acción de amenazar, hostigar, humillar o molestar, llevadas a cabo por un adulto contra otro por medio de las TIC, es lo que se conoce como ciberacoso (Pantallas Amigas, 2016). Y este ciberacoso resulta mucho más grave cuando implica a menores. Se ha realizado una clasificación de los principales tipos del acoso a menores, que son las que nos preocupan en este documento.

*Cyberbullying.*

Este acoso es lo que tradicionalmente consideramos *bullying*. Este hostigamiento se lleva a cabo por medios electrónicos: e-mail, mensajería instantánea, redes sociales, publicación de vídeos o fotografías, etc. (Durán & Martinez-Pecino, 2015).

Los recientes avances en la tecnología informática han ayudado a los depredadores sexuales en sus depravaciones con la intención de explotar a los niños (Hinduja & Patchin, 2011). A medida que la esfera digital se expande se ha vuelto cada vez más común, especialmente entre los adolescentes, que al *bullying* físico en el aula se sume el virtual, sometiendo al menor a un acoso de 24 horas (Cherian, 2019). Se trata de un acoso por parte de iguales en el contexto de las TIC (Lenhart, 2007). Puede incluir desde el chantaje a humillaciones, insultos o difusión de contenidos amenazantes entre los menores (Dehue, Bolman, Vollink, & Mieneke, 2012).

La intimidación y las burlas a través de las redes sociales es la razón por la que muchos menores no quieren levantarse por la mañana, generándoles graves secuelas físicas, a veces auto infligidas, y psicológicas.

*Cyberbullying con intención sexual: grooming.*

Este tipo de acoso es ejercido por un adulto (Craven, Brown, & Gilchrist, 2006). Su término anglosajón es *child grooming* (Whittle, Hamilton-Giachritsis, Beech, & Collings, 2013). Son acciones encaminadas a fabricar una relación y un control emocional sobre el menor, para crear un ambiente propicio para su posterior abuso sexual. Es decir, se prepara al niño, estableciéndose una conexión emocional con él y a veces con la familia, para reducir su resistencia en un futuro abuso físico. Es un acoso con un contenido, explícito o implícito, de tipo sexual (Montiel, Carbonell, & Pereda, 2016).

Las webs de anuncios de Internet, las salas de chat y los sitios web privados, están siendo utilizados diariamente por pedófilos para conocer a niños desprevenidos. A ello hay que sumar la falta de mecanismos a nivel internacional que frene el contenido y las actividades ilegales. Aunque muchos países disponen de leyes que protegen a los niños, es necesario una legislación internacional para combatir el abuso sexual infantil (Kierkegaard, 2008).

En España, con la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Boletín Oficial del Estado, 2015), en relación a delitos contra la libertad sexual y protección de menores, se introduce el artículo 183 ter, para proteger a los menores de dieciséis años, castigando al que trate de contactar con éstos, mediante Internet u otras TIC, con la intención de realizar los actos que describen los arts. 183 y 189. En el segundo apartado del artículo 183 ter, se indica que se castigue al que utilice esos medios con el propósito de engatusar al menor, para que así éste le proporcione imágenes suyas de carácter

pornográfico. También se modifica el artículo 189, donde se incluye en el apartado 1 la definición de pornografía infantil. Además de castigar la adquisición o tenencia de pornografía infantil, se incluye un apartado que sanciona al que accede por medio de las TIC con conocimiento a este tipo de pornografía (Mesa Millán, 2017).

*Cyberstalking.*

Es otro tipo de acoso cibernético para acechar u hostigar a un individuo, grupo u organización (Pires, Sani, & Soeiro, 2018). Puede incluir acusaciones falsas, calumnias y difamación. También puede incluir la amenaza, manipulación y destrucción de datos, *phishing* y el seguimiento de la víctima. Y claro, esto también se puede aplicar en el ámbito de los menores.

*Sexting.*

De la unión de dos anglicismos "*sex*" y "*texting*" ((Patchin & Hinduja, 2020); (Drouin & Landgraff, 2012)). Las nuevas capacidades de los dispositivos ha conducido a que también se aplique el envío, no sólo a través de Smartphone sino mediante cualquier soporte digital, de contenido sexual multimedia, tomado o grabado por el protagonista ((Wittes, Poplin, Jurecic, & Spera, 2016); (Ahern & Mechling, 2013); (Gordon-Messer, Bauermeister, Grodzinski, & Zimmerman, 2013); (Wolak, Finkelhor, Walsh, & Treitman, 2018)).

La conducta lesiva, que deriva a su vez en *cyberbullying*, tiene lugar si el que recibe el contenido audiovisual, o porque le ha llegado de manos de su protagonista, o porque lo ha obtenido por medios ilegales, lo envía a terceras personas o lo hace circular de manera libre generando un daño psicológico y moral.

En ocasiones se le suma un componente económico. Se trata de amenazar a la víctima con la difusión por un motivo meramente monetario. Todo ello debería ser notificado a las autoridades, dado que estas conductas llevan aparejadas implicaciones penales.

Asociado a *sexting* tenemos el *sexcasting*, que se asocia con la grabación de contenidos sexuales a través de la cámara web y difundido por mensajería, email, etc., y la sextorsión, derivado del término inglés *sextortion*. Es una forma de explotación sexual donde se chantajea por medio de una imagen compartida a través de Internet (*sexting*), donde la víctima es coaccionada para mantener relaciones sexuales con quien la chantajea. A veces usada para producir pornografía, o bien una extorsión económica o cualquier otro tipo de coacción puntual o continuada. Son numerosos los casos denunciados de chantajistas detrás de los cuales se halla un exnovio.

*Bofetada feliz o happy slapping.*

Se define como una práctica por la cual un grupo de personas ataca a un extraño al azar mientras filma el incidente en un dispositivo móvil, para hacer circular las imágenes o publicarlas en línea.

Es una acción para humillar, en la que un grupo de menores agrede a otro (Palasinski, 2012). La manera es por medio de una bofetada inesperada y fuerte, de ahí el término inglés *happy slapping* (Montiel et al., 2016). Otras variantes pueden ser un tirón de pelo, una patada o cualquier otra forma de agresión física o vejación. Los menores lo hacen como parte de un reto (Mann, 2009). Se graba y posteriormente se difunde. En el ámbito escolar esta agresión, en principio puntual, puede tener continuidad y derivar en *cyberbullying*, por lo que supone de humillación al menor.

*Cyberbaiting.*

En esta modalidad de acoso la víctima es el docente y el agresor, o agresores, son menores. Es un *cyberbullying* en el que se hostiga de forma psicológica y reiterada al docente para denigrarlo. Este nuevo contexto de acoso a los docentes, a través de la Red, tiene su origen en las acciones de vandalismo y humillación a los que someten ciertos alumnos problemáticos a sus profesores, que incluye desde la agresión física a la destrucción de sus bienes materiales. Estos comportamientos generan estrés y depresión con graves secuelas psicológicas y morales.

*Fake news.*

Las noticias falsas consisten en desinformación deliberada o mentiras difundidas a través de los medios tradicionales o las redes sociales en línea (Lazer et al., 2018).

Igual que se difunden bulos sobre un alumno en las aulas con la intención de *bullying*, resulta realmente eficaz la Red para la propagación de infundios.

El cotilleo trae beneficios personales y sociales. Necesitamos tener información sobre otras personas. El chismorreo es una interacción social y facilita las relaciones dentro del grupo, permitiéndonos iniciar conversaciones incluso con gente a la que no conocemos. Las noticias falsas, en este caso chismorreos inventados para manchar la imagen de otro, van por el mismo camino. Resulta divertido, pero sólo para la persona que los lee y escucha, no para el protagonista del infundio.

## 4. Elementos empleados en el acoso a través de medios tecnológicos.

Cada uno de nosotros tienen mayor o menor cultura digital. En la Red todos nos convertimos en víctimas, puesto que somos sujetos pasivos potenciales de los ciberdelincuentes. Por ello la necesidad de una mayor demanda social en ciberseguridad a las Autoridades. Los Gobiernos de los países deben preocuparse legislando, siendo siempre garantes de nuestros derechos.

Los medios tecnológicos con los que los menores sufren o acosan a sus iguales son numerosos. La proliferación de los dispositivos y sus variadas aplicaciones de audio, foto y vídeo ha hecho que los abusadores de toda la vida sean también muy creativos, haciendo uso de estas tecnologías en sus ataques a menores. Analizamos ahora algunos medios de ciberacoso (Ojeda Martinez, 2018).

*Mensajería instantánea, chats públicos, foros y correo electrónico.*

Los correos electrónicos, los mensajes de texto y las redes sociales ofrecen comunicación instantánea a una sociedad que vive acelerada. Es un medio rápido y efectivo y disponemos de multitud de plataformas. Como todo, este tipo de innovación cuenta con detractores y seguidores. Estas aplicaciones facilitan las comunicaciones entre los menores. Son gratuitas, amigables y fáciles de implementar en los móviles. Además, apenas consumen datos, con lo que el gasto es mínimo si tienen restricciones.

Suele ser relativamente sencillo, si se conoce como hacerlo, rastrear un e-mail hasta la fuente con toda la información posible. De esta manera podremos averiguar quién hay detrás de un correo. Es una manera eficaz de asegurar la veracidad del remitente. Incluso podemos utilizarlo para bloquear una fuente de origen que no cesa en sus envíos. El problema es que un mismo usuario puede generar miles de direcciones

diferentes del correo en origen, de forma que el filtro de nuestro servidor no sea capaz de eliminarlo.

Si analizamos el mensaje en origen, la información que aparece en *From* a priori nos indica el remitente del mensaje, algo que es sencillo de falsificar. Para rastrear la dirección IP del remitente original del correo electrónico, hay que ir al primer *Received* en el encabezado completo del correo electrónico. Junto a la primera línea *Received* está la dirección IP del servidor que envió el e-mail. A veces esto aparece como *X-Originating-IP* o también *Original-IP* (Javier Jiménez, 2018).

*Smartphone y otros dispositivos multimedia.*

La aparición de estos dispositivos con potentes cámaras supone un nuevo medio para el acoso y la intimidación. El hecho de contar con un dispositivo móvil capaz de captar imágenes en formato digital, y remitirlas inmediatamente a todos los contactos, hace que cualquier imagen lesiva contra un menor se pueda difundir de forma inmediata entre un gran número de personas.

Lo que surge como una foto inocente o un vídeo alojados en un dispositivo, pasa a ser difundido de forma masiva, logrando que el efecto dañino buscado por el acosador conlleve un mayor impacto.

*Redes sociales.*

Estas plataformas permiten a los usuarios la interacción. Facebook, Twitter e Instagram siguen siendo las comunidades más grandes y con mayor reconocimiento. Y son un escaparate al que los más exhibicionistas les gusta asomarse. Pero igual que una Red puede dar prestigio, también puede tumbar una reputación. Ofrecen la posibilidad de publicar vídeos e imágenes, siendo visionado este perfil del sujeto por millones de seguidores en todo el mundo. Es en este tipo de redes donde se dan un elevado número de acosos online y donde los jóvenes son los más vulnerables.

Los menores emplean estas redes sociales como un medio para intercambiar impresiones y comunicarse con sus compañeros. El alto grado de difusión de las redes sociales, y la posibilidad de publicación de fotos y vídeos, hacen de estas plataformas un escenario atractivo para los acosadores.

## 5. Recomendaciones dirigidas a los menores cuando se conectan a la Red.

Es necesario plantear la necesidad de ser cuidadosos con los datos que publicamos en los perfiles de las redes sociales, o los que se proporcionan a través de los servicios de mensajería instantánea. En la Red los menores deben comportarse con responsabilidad, respeto y sentido común, igual que lo hacen en el mundo real.

Entre las medidas que se sugiere adoptar:

- Recurrir al uso de motes o seudónimos para navegar en la Red. Esta identidad digital no debe comprometer la seguridad personal y profesional de quien la usa. Será conocido únicamente por su círculo de contactos que saben el mote que emplea en Internet.

- Ser cuidadoso con los datos que se publican. No publicar demasiada información personal en Internet que podría ser utilizada contra el menor o su entorno.
- No publicar más información de la necesaria y, en caso de datos como el correo electrónico o teléfono móvil, hacerlo de la forma más privada posible.
- Evitar la publicación de contenidos audiovisuales, dado que pueden comprometer y poner en riesgo la privacidad e intimidad de personas de su entorno. Los padres no son conscientes de que publican toda la vida de sus hijos en la web y no saben quién está al otro lado observando.
- Siempre que se vayan a alojar contenidos de este tipo o información relativa a terceros, notificarlo previamente al interesado para su autorización o, en su caso, filtrar los contenidos.
- No agregar como contacto a desconocidos. Especialmente es crítico este punto en lo que respecta a los menores. Para asegurarse, en caso de que el nombre de usuario no sea reconocible, puede preguntar a sus contactos si es conocido por ellos (amigos comunes, compañeros de colegio/instituto, etc.). Si se identifica alguna conducta malintencionada, o se dan discrepancias entre el perfil declarado y el real, bloquearle. En función de la gravedad de la situación, es recomendable ponerlo en conocimiento de la plataforma y de las autoridades competentes. En estos casos siempre conviene que lo comunique a sus amigos, para que estén prevenidos ante ese sujeto.
- Evitar el envío de imágenes o vídeos a usuarios en los que no se confía. En caso de que un contacto desconocido intente involucrarse de forma muy temprana en nuestra vida social, y al poco tiempo solicite que se le envíe una foto o encender nuestra cámara web, es mejor dudar y en un momento posterior disculparse, a ser afectado por alguna de las conductas mencionadas.
- Si se percibe o detecta una situación de riesgo, o en la que un tercero comience a solicitar temas relacionados con aspectos sexuales, se debe comunicar inmediatamente a los padres o tutores legales.

En el ámbito docente, el uso de plataformas de videoconferencia que permiten la interacción entre alumnos y profesores, mediante chat o registro de imagen o voz, puede suponer una identificación de los estudiantes. La intervención en la clase debe regirse por los principios del funcionamiento ordinario de la docencia, y no requiere del consentimiento del estudiante. Las grabaciones que se hagan de la videoconferencia para su posterior acceso a través del campus virtual, únicamente pueden ser utilizadas en ese contexto, durante el curso y en el periodo asignado al mismo. El uso de las grabaciones fuera del ámbito de la docencia en el aula virtual no es legítimo. Cualquier difusión no autorizada genera responsabilidades administrativas, civiles y penales a la persona infractora.

## 6. Mecanismos para la prevención del ciberacoso.

Internet ofrece la sensación de anonimato. Y es cierto que quien quiere ocultarse lo hace, siendo muy difícil sacar a la luz al que sabe cómo esconderse o se mueve en la Deep web. Pero afortunadamente no todos los que ofenden o lesionan a nuestros menores son expertos en la Red. Existen medios tecnológicos suficientes para poder determinar el lugar exacto y el equipo informático desde el que se llevó a cabo el presunto delito. Por ello velan y trabajan los expertos informáticos de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE).

Cuando uno se conecta a la Red lo hace gracias a la dirección IP que proporciona el Proveedor de Servicios de Internet. La IP, ya sea estática o dinámica, funciona como una matrícula que permite la identificación de los equipos que la usan y conocer la identidad de la conexión. Este dato, que únicamente puede ser conocido y utilizado previa solicitud judicial, permite perseguir el ciberdelito en sus diferentes variantes. Para averiguar la identidad de los presuntos acosadores, junto a la dirección IP, con frecuencia las investigaciones de los FCSE emplean servicios públicos de Internet, como buscadores, redes sociales, programas de mensajería instantánea, etc.

En lo que respecta a la Unión Europea se han dado pasos para la prevención a nivel internacional. *European Union Agency for Law Enforcement Cooperation* (EUROPOL), es la agencia de aplicación de la ley de la Unión Europea. Destaca el proyecto *Joint Cybercrime Action Task Force* (J-CAT) (EUROPOL, n.d.), o Grupo de Trabajo Conjunto de Acción contra el Cibercrimen. Se encuadra en la Unidad de lucha contra el Cibercrimen de Europol, conocida como *European Cyber Crime Center*, o por sus siglas, EC3. El proyecto J-CAT cuenta con especialistas de los tres departamentos de analistas que forman el EC3: *malware* y *hacking*, fraudes en medios de pago y explotación sexual de menores.

En España, dentro del Grupo de Delitos Telemáticos, existen operativos tanto dentro de la Guardia Civil como en la Policía Nacional y diversos grupos locales. Se ha adoptado el esquema de trabajo que deriva del Convenio sobre ciberdelincuencia del Consejo de Europa de 2001 (Council of Europe, 2001), y el protocolo adicional firmado dos años después para incluir los delitos de apología del racismo y la xenofobia. Una de las 4 grandes líneas que investiga es la relacionada con los contenidos de menores, como son la pornografía infantil, abusos sexuales a menores, *cyberbullying*, etc.

*Consejos para el menor.*

Se dice con toda la razón que el mejor secreto es aquel que no se cuenta a nadie. En el momento que se verbaliza a un segundo nunca, o casi nunca, tendrás la certeza de que ese interlocutor no se lo cuente “en confianza” a un tercero.

Pero si bien hay mecanismos para paliar el daño, lo adecuado sería la prevención del mismo. Y en ese sentido debemos implicar a todos los actores de la sociedad para que velen por los menores. Pero, ¿cómo prevenir?

- Debemos hacer conscientes a los menores de las consecuencias de compartir información. No son conocedores del alcance y visibilidad de todo lo que publicamos a través de Internet y su capacidad de divulgación. En el momento que una imagen, un vídeo, un tuit, etc. está en la Red, queda fuera del control de quien lo lanza. Podemos borrarlo o puede ser eliminado por imperativo legal con una orden de un juez, pero eso no impedirá que lo que se ha compartido en una ocasión, vuelva a ser lanzado y compartido por terceros. Una vez que se ha pulsado la tecla de envío, no hay marcha atrás. Imposible tener la certeza de que la persona que recibe el documento, la foto, el vídeo, el tuit, el mensaje, los mantendrá en la privacidad. Puede incluso que por error o una acción malintencionada de terceros, esa imagen pase a ser de dominio público.
- El conocimiento de las herramientas nos facilitará configurar de forma adecuada y personalizada la privacidad de las redes sociales. Si bien es cierto que algunas redes sociales limitan la edad en las condiciones del acceso, el menor puede engañar diciendo que tiene más edad biológica. Podemos pedir ayuda a personas expertas para configurar la privacidad y que nos asesoren ante las dudas.

- No se debe facilitar datos personales a extraños que les sirva para crackear nuestro dispositivo, ya sea para acceder a nuestras redes sociales y alterarlas o robar información sensible.
- Hay que seguir un código ético y de conducta respetuoso en lo que publicas, bien sea información personal o aportaciones en los tablones de otros usuarios.
- Desarrollar el pensamiento crítico. Analizar y cuestionar la realidad, tomando decisiones propias. No te sumes a lo que otros opinan por el hecho de ser tus amigos si no compartes sus opiniones.
- Cuidar y mantener las relaciones sociales. Tus amigos y familia son tus mejores aliados a la hora de protegerte. No es probable que te traicionen en la Red si no lo harían en la vida real.
- Fomentar la empatía en tus relaciones.
- Evitar publicaciones cuando tu estado de ánimo esté alterado para evitar tuits inconvenientes.
- Si detectas situación de acoso a tu alrededor, observa y ofrece ayuda. El acosado a veces no verbaliza su angustia. Ponlo en conocimiento de un adulto responsable y ayuda a buscar una posible solución al problema.

En el caso de que el ciberacoso se haya producido, ¿cómo actuamos?

- Claramente ponlo en conocimiento de un adulto responsable que te ayude a gestionar el problema de la forma más adecuada. Si es grave, pide ayuda con urgencia.
- No difundas imágenes o grabaciones audiovisuales de otros sin su permiso que menoscaben su intimidad. En España hay sentencia, dictada por la Sala Segunda del Tribunal Supremo, en relación al artículo 197.7 del Código Penal, introducido tras la reforma de 2015. Dicho artículo (Boletín Oficial del Estado, 2015) establece en la página 65 que:

  > *"Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses al que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona".*

- No contestes a las provocaciones, el abusón se retroalimenta del miedo, la vergüenza y la ira del abusado.
- Si te molestan, abandona la Red. A veces poner distancia es bueno para la salud física y mental.
- Guarda las pruebas del acoso y denuncia a través del administrador del servicio Web (Facebook, Instagram, Twitter, LinkedIn, Google+, etc.) para que evalúe y elimine el contenido lesivo.
- No te sientas mal por la situación. El resolver el problema te hará a la larga más fuerte. Si necesitas gestionar tus emociones puedes hablar con un especialista para comunicar lo que piensas de forma asertiva, pidiendo lo que quieres y verbalizando lo que no te gusta.

El acceso de los menores a la Red, sin control parental en la gran mayoría de los casos, y el acceso a contenidos altamente violentos y de carga sexual elevada, ha permitido que se normalice en la psique del menor esas imágenes. En el fondo sabe que esos contenidos no son adecuados a su franja de edad. Por eso los ve en gran medida a escondidas. Pero a veces esas webs dan acceso a otros peligros que les

exponen a depredadores sexuales. En casos de ciberacoso con intención sexual se pueden tomar, no obstante, precauciones.

- El menor debe aprender con qué personas tiene que relacionarse a través de estos medios, y cómo no llevar a cabo acciones como concertar citas con extraños en la vida real o al menos no hacerlo sin la presencia de un adulto.
- Inculcar en los menores la necesidad del respeto por la privacidad de uno mismo y de los demás. Si son conscientes de los riesgos existentes decidirán de forma más reflexiva con quien lo hacen.
- Hablar con el menor de forma razonada. Desde una actitud de asertividad y empatía hay que debatir los riesgos y los casos de actualidad, a la vez que se genera un ambiente de confianza que facilite que el menor exponga sus ideas y problemas y así reflexione sobre las consecuencias.

En el caso de ser consciente de la existencia de alguna de estas conductas de ciberacoso, es recomendable adoptar las siguientes medidas:

- Mantener las evidencias del acoso en cualquiera de sus modalidades para poder presentarlas a la Autoridad competente. Pueden ser desde contenidos multimedia, SMS, correos electrónicos, etc. Será la prueba que justifique una posterior condena del infractor.
- Denunciar el acoso a las FCSE, que disponen de unidades de delitos informáticos.
- Identificar al acosador. Hay que averiguar la dirección IP. Para ello se puede contar con las FCSE, con medios para este tipo de búsquedas.
- Contactar con la compañía del medio empleado para cometer el acoso (compañía de teléfono, propietario del dominio o sitio web, etc.). Será necesaria una orden judicial para que la compañía ofrezca a las FCSE este tipo de información confidencial.
- En caso de *cyberbullying*: si éste procede del entorno escolar, habrá que tomar tres medidas adicionales, en primer lugar, ponerlo en conocimiento de la dirección de escuela para recibir el apoyo necesario, seguidamente recurrir a las organizaciones especializadas en acoso de la zona escolar y, por último, contactar con los padres del agresor para tratar de mediar y solucionar el conflicto. De ser necesario deben aplicarse las medidas disciplinarias ajustadas al delito.

*Consejos para los adultos.*

- Es necesario trasladar confianza al menor para que ante una incidencia en la Red recurra al adulto. En las escuelas suelen contar con la intervención de las FCSE para impartir charlas en el aula, tanto a los padres como a los alumnos y docentes, donde además de la prevención y mejor gestión del problema, se fomenta la confianza para acusar el delito e informan de los recursos que pueden ser consultados.
- Involucrarse en el uso que los menores hacen de Internet. La brecha digital existente entre adultos y niños puede hacer que los padres se mantengan alejados de la realidad virtual en la que viven los menores y adolescentes, para los cuales el uso de las herramientas de la web 2.0 es parte de su vida cotidiana. Esto provoca que, en ocasiones, los padres no consigan comprender las consecuencias que un mal manejo de la tecnología puede tener para sus hijos.
- Es importante que el ordenador se encuentre en algún sitio común de la casa, permitiendo de esta forma que los padres pueden conocer, en cierto modo, el uso que los menores hacen de la web: utilización de servicios, acceso a

determinados contenidos, frecuencia de conexión, duración de las sesiones, etc., sin que esto implique una intromisión en la intimidad del menor.

- Establecer un horario de uso de Internet. Las nuevas tecnologías han cambiado la forma de comunicación entre jóvenes: las redes sociales y plataformas colaborativas son puntos de encuentros públicos y masivos. Es necesario marcar pautas de utilización claras sobre duración o momento de la conexión, aplicaciones, etc. El control parental es muy útil en estos casos.
- Impulsar el uso responsable de la cámara web. En la mayoría de los dispositivos móviles viene instalada. Se denuncian cada vez más casos en que se ha activado de forma remota el vídeo o el micrófono de la cámara con la finalidad de escuchar y grabar momentos íntimos. Una buena opción es taparla con el propósito de cubrirla cuando no se use, obstaculizando la grabación en caso de ser activada de modo remoto.
- Los adultos, más que el control del menor, buscan la seguridad. No se trata de que se sientan controlados y coartados: este control debe ser realizado de la forma menos intrusiva posible en su intimidad. Conviene establecer un control parental que garantice información acerca de con qué usuarios y en qué ámbito se comunican los menores. Entre las más conocidas están (1) Spyzie, para sistema operativo iOS y Android ("Spyzie," n.d.); (2) K9 Web Protection, desarrollada para Windows y macOS, solía ser un servicio pago, y aunque ya no se actualiza, la versión gratuita todavía está disponible (Blue Coat Systems, n.d.); (3) Avira, es una aplicación de seguridad gratuita que incluye un antivirus; (4) Qustodio Control Parental Free (Cruz, Gaspar, & Gabel, 2012), facilita el análisis completo de informes, el rastreo del dispositivo fiscalizado en tiempo real, el filtrado de contenido adulto y la monitorización de la actividad en redes sociales; y (5) KidLogger, que rastrea todo tipo de datos, como las pulsaciones de teclas en los dispositivos, incluidas las plataformas como Skype y las redes sociales.
- Para los menores y no tan jóvenes los selfis son su manera de presentarse a los demás, en gran parte para fardar, pero también para expresar cómo se sienten. Cualquier contenido es susceptible de ser interpretado y malinterpretado. Ni que decir tiene que no se deberían enviar fotos ni vídeos personales a ningún desconocido.
- Establecer un diálogo permanente con los menores y adolescentes es tarea fundamental de padres, tutores y docentes. La comunicación debe abordar tanto los aspectos positivos del uso de la tecnología, como los posibles riesgos que Internet puede implicar. Sólo con un conocimiento riguroso de las situaciones que pueden tener lugar en Internet es posible estar preparado para responder a ellas.

## 7. Conclusiones.

El uso de las TIC, y todas las aplicaciones que nos ofrecen hoy en día, nos facilitan la comunicación ágil y dinámica para mantener el contacto con familiares, amigos o el entorno profesional. Pero no sólo son usadas por los adultos. Nuestros jóvenes no entienden el mundo sin ellas. La Red es el nuevo contexto en el que nos movemos y que engloba prácticamente todos los aspectos de la vida. Los menores pueden sufrir, por parte de compañeros o de adultos, una amplia gama de ataques que pueden afectar a su honor, intimidad, libertad o dignidad.

La jurisprudencia ha reconducido a distintos tipos penales muchas de las conductas que, con poca precisión, podríamos denominar de acoso a menores a través de Internet.

Y lo ha hecho, como no podría ser de otra forma, a partir de los distintos bienes jurídicos de los menores dañados o puestos en riesgo por los ciberataques. El honor, la libertad, la intimidad, entre otros bienes de los menores que pueden ser afectados, delimitarán la concreta respuesta jurídica.

Ante las situaciones de riesgo descritas a lo largo del documento, el papel que juegan los padres o tutores de los menores es crucial. Éstos, con independencia de controlar y establecer medidas y normas de uso en Internet, deben ser conscientes de que pueden actuar con inmediatez en dos líneas prioritarias: procurar la seguridad del menor, evitando que continúe manteniendo cualquier tipo de relación con el acosador, y denunciar los hechos ante las FCSE, que darán traslado a los grupos especializados en delitos informáticos para que sea investigado el caso en cuestión.

El principal consejo a los padres es que, también en Internet, sean el mejor ejemplo para sus hijos. Si observan que ponemos una foto sexy, por imitación harán lo mismo. Si ve que cuidamos nuestra reputación digital, también lo harán ellos y se evitarán problemas en un futuro. Lo ideal sería crear entornos TIC seguros adaptados a cada edad y cada momento de madurez. No funciona fiscalizar las actividades de los hijos, se trata de ofrecerles recursos y pensamiento crítico frente a los posibles riesgos de la Red. Explicarle qué son los ajustes de privacidad, cómo sospechar de perfiles falsos, cómo tapar la webcam, por qué no podemos fiarnos de correos electrónicos que nos piden contraseñas y datos bancarios, ni subir ni difundir fotos de menores en las redes sociales.

## Agradecimientos

Este trabajo no hubiera sido posible sin el apoyo proporcionado por el Vicerrectorado de Docencia de la Universidad de Valladolid (Proyecto de Innovación Docente Nº 128).

## Referencias

Ahern, N. R., & Mechling, B. (2013). Sexting: Serious problems for youth. *Journal of Psychosocial Nursing and Mental Health Services*. https://doi.org/10.3928/02793695-20130503-02

Blue Coat Systems. (n.d.). K9 Web Protection. Retrieved April 15, 2020, from https://k9-web-protection.en.softonic.com/

Boletín Oficial del Estado. (2015). Ley Orgánica 1/2015. Retrieved April 15, 2020, from https://www.boe.es/boe/dias/2015/03/31/pdfs/BOE-A-2015-3439.pdf%0D

Cherian, V. E. (2019). Cyberbulling. *Research Journal of Science and Technology*. https://doi.org/10.5958/2349-2988.2019.00011.1

Consejo General de la Psicología de España. (2019). El uso de las nuevas tecnologías entre los menores se encuentra muy extendido, según el INE. Retrieved April 14, 2020, from http://www.infocop.es/view_article.asp?id=8362

Council of Europe. (2001). Convention on Cybercrime. Retrieved April 15, 2020, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Craven, S., Brown, S., & Gilchrist, E. (2006). Sexual grooming of children: Review of literature and theoretical considerations. *Journal of Sexual Aggression*.

https://doi.org/10.1080/13552600601069414

Cruz, E., Gaspar, J., & Gabel, J. (2012). Qustodio. Retrieved April 15, 2020, from https://www.qustodio.com/es/

Dehue, F., Bolman, C., Vollink, T., & Mieneke, P. (2012). Cyberbulling and traditional bulling in relation to adolescents' preception of parenting. *Journal of Cyber Therapy and Rehabilitation*.

Díaz, V. P., la Rosa, I. Q., Durán, G. R., Gil, Z. F., Pavón, T. L., Hechavarría, O. P., & Valdés, M. M. (2011). Impact of the information andc ommunication technologies in education and new paradigms in the educational approach. *Revista Cubana de Educacion Medica Superior*.

Drouin, M., & Landgraff, C. (2012). Texting, sexting, and attachment in college students' romantic relationships. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2011.10.015

Durán, M., & Martinez-Pecino, R. (2015). Cyberbullying trough mobile phone and the internet in dating relationships among youth people. *Comunicar*. https://doi.org/10.3916/C44-2015-17

EUROPOL. (n.d.). Joint Cybercrime Action Taskforce (J-CAT). Retrieved April 15, 2020, from https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

Gordon-Messer, D., Bauermeister, J. A., Grodzinski, A., & Zimmerman, M. (2013). Sexting among young adults. *Journal of Adolescent Health*. https://doi.org/10.1016/j.jadohealth.2012.05.013

Hinduja, S., & Patchin, J. W. (2011). Cyberbullying research summary: Bullying, cyberbulling and sexual orientation. In *Cyberbulling Research Center*. https://doi.org/10.1111/j.1746-1561.2010.00548.x

Javier Jiménez. (2018). Cómo rastrear un e-mail hasta la dirección IP de origen en Gmail y Outlook. Retrieved from https://www.redeszone.net/2018/08/25/rastrear-e-mail-direccion-ip-origen-gmail-outlook/

Kierkegaard, S. (2008). Cybering, online grooming and ageplay. *Computer Law and Security Report*. https://doi.org/10.1016/j.clsr.2007.11.004

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., … Zittrain, J. L. (2018). The science of fake news. *Science*. https://doi.org/10.1126/science.aao2998

Lenhart, A. (2007). Cyberbulling and Online Teens. *Pew Internet & American Life ProjectAmerican Life Project*.

Mann, B. L. (2009). Social networking websites - A concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos. *International Journal of Law and Information Technology*. https://doi.org/10.1093/ijlit/ean008

Mesa Millán, A. (2017). La ciberdelincuencia y sus consecuencias jurídicas. Retrieved April 15, 2020, from http://uvadoc.uva.es/handle/10324/26749

Miró Llinares, F. (2013). La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio. *Revista Española de Investigación Criminológica: REIC*.

Montiel, I., Carbonell, E., & Pereda, N. (2016). Multiple online victimization of Spanish adolescents: Results from a community sample. *Child Abuse and Neglect*. https://doi.org/10.1016/j.chiabu.2015.12.005

Ojeda Martinez, L. (2018). *Análisis y soluciones para la prevención de la violencia*

*ejercida a través de las TIC en jóvenes y niños*. Retrieved from http://uvadoc.uva.es/handle/10324/30587

Palasinski, M. (2012). Implications of urban adolescent discourses of (un)happy slapping. *Safer Communities*. https://doi.org/10.1108/17578041211244076

Pantallas Amigas. (2016). Acoso escolar – Ciberacoso entre iguales.

Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse: Journal of Research and Treatment*. https://doi.org/10.1177/1079063218800469

Pires, S. A., Sani, A. I., & Soeiro, C. (2018). Stalking e ciberstalking em estudantes universitários: Uma revisão sistemática. *Revista Portuguesa de Investigação Comportamental e Social*. https://doi.org/10.31211/rpics.2018.4.2.75

Prensky, M. (2014). Digital Natives, Digital Immigrants. In *From Digital Natives to Digital Wisdom: Hopeful Essays for 21st Century Learning*. https://doi.org/10.4135/9781483387765.n6

Spyzie. (n.d.). Retrieved April 15, 2020, from www.spyzie.com%0A

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior*. https://doi.org/10.1016/j.avb.2012.09.003

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). Sextortion: Cybersecurity, teenagers, and remote sexual assault. *Centre for Technology Innovation*.

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of Minors: Characteristics and Dynamics. *Journal of Adolescent Health*. https://doi.org/10.1016/j.jadohealth.2017.08.014