Ciberacoso y Ciberbullying II

En el post anterior hablábamos de ciberacoso, su definición, características y perfiles. No obstante es importante finalizar el artículo sobre este delito ampliando la información a las Formas de Acoso, normativa legal aplicable y el procedimiento de actuación en caso de ciberacoso.

Formas de acoso

El acoso, definido en general como cualquier forma de maltrato, psicológico, verbal o físico de forma reiterada y reproducido a lo largo del tiempo, se puede iniciar de diversas maneras:

- Por una situación dada en un momento y tiempo concretos.
- Parte de una mentira. Atribuir a alguien un hecho falso y acusarle permanentemente de ser lo que no es
- Debido a una característica física distintiva que se aprovecha para ridiculizar al acosado

Las formas de acoso que se pueden concretar en el ciberacoco o ciberbullying se resumen en:

- Hostigamiento: envío de imágenes denigrantes, seguimiento a través de software espía, envío de virus informáticos, etc.
- Exclusión: uso de entornos públicos para acosar y mandar comentarios despectivos o difamatorios con el objetivo de provocar una respuesta expansiva, denegación del acceso a foros, chats o plataformas sociales de todo el grupo a la víctima, etc.
- Manipulación: uso de información encontrada en las plataformas para difundirla de forma no adecuada entre los miembros, acceso con la clave de otra persona a un servicio y realización de acciones que puedan perjudicarle en su nombre, etc.

Algunas de las manifestaciones más frecuentes del ciberacoso, aunque considerando las posibles variaciones según cada entorno o grupos son:

- Envío repetido de mensajes ofensivos e insultantes hacia un determinado individuo.
- Luchas online a través de mensajes electrónicos (chat, mensajería instantánea vía móvil, SMS, redes sociales…) con un lenguaje enfadado y soez.
- Envío de mensajes que incluyen amenazas de daños altamente intimidatorios, acompañadas además de otras actividades en la red (acecho, seguimiento), que hacen que la persona tema por su propia seguridad.
- Enviar o propagar cotilleos crueles o rumores sobre alguien dañando su reputación.
- Pretender ser alguien que no se es y enviar o difundir materiales e informaciones online que dejan en ridículo a la persona en cuestión, la ponen en riesgo o causan daño a su reputación ante sus conocidos y/o amigos.

- Compartir online información secreta o embarazosa de alguien. Engañar a alguien para que revele información secreta o embarazosa que después se comparte online. Publicación de datos personales, etc.
- Excluir intencionalmente a alguien de un grupo online, como una lista de amigos.
- Enviar programas basura: virus, suscripción a listas de pornografía, colapsar el buzón del acosado etc.
- Grabar y colgar en Internet vídeos de peleas y asaltos a personas a quienes se agrede y que después quedan expuestas a todos.
- Utilizar un blog personal para denigrar y hablar mal de una persona.
- Manipular materiales digitales: fotos, conversaciones grabadas, correos electrónicos, cambiarlos, trucarlos y modificarlos para ridiculizar y dañar a personas.
- Robar contraseñas para suplantar su identidad.
- Realizar y/o participar en encuestas y rankings en Internet denigratorias para algunas personas .

- Guía de Actuación contra el ciberacoso – Chaval.es

Normativa legal

Desde el punto de vista legal, el tipo penal más próximo al ciberacoso es el que se recoge en los artículos 197 y 510 del Código Penal (en adelante CP). Allí se detalla la revelación de información a terceros sin consentimiento del titular, la posibilidad de que la víctima sea un menor o un incapaz, y el uso de las TIC para lesionar la dignidad de las personas mediante acciones que entrañen humillación, menosprecio o descrédito:

Cualquier acto de ciberacoso, la finalidad de lesionar o avergonzar es fundamental. En realidad, estas modalidades delictivas deben encuadrarse en los delitos contra la integridad moral, pues en todos los casos lo que se pretende atacar es la dignidad de la persona. La referencia a la dignidad personal es cita ineludible a la hora de proponer cualquier definición de ciberacoso.

El Ministerio de Industria Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información y la entidad pública Red.es ha publicado un curso sobre Ciberbulling o Ciberacoso. En el mismo se ha redactado un monográfico en el que se describe el delito, el riesgo, los métodos y medios para

llevarlo a cabo. http://formacion.chaval.es/component/jdownloads/send/2-contenidos-ciberbullying/15-monografico-ciberbullying

En dicho monográfico en la página 3 se define Ciberbulling o Ciberacoso *como «la acción de acosar a otra persona mediante el uso de medios digitales».*

En el apartado 2 Conceptualización y descripción del riesgo se detallan las principales características del ciberacoso. Que son.

1.- Se busca causar daño

2.- Se realiza de forma intencional

3.- Se realiza de forma repetida

4.- Se utilizan medios digitales

Del mismo modo el monográfico en la página 5 describe los métodos y medios para cometer ciberbullying

[…] los métodos y medios más representativos actualmente incluyen:

- ***Ataques directos**: insultos o amenazas enviadas directamente a la víctima a través de redes sociales, mensajería instantánea y correo electrónico. Robo de contraseñas para el secuestro y cierre de perfiles en redes sociales y otros servicios web, y para el robo de recursos en juegos en línea. Envío de virusinformáticos para manipular el ordenador de la víctima.*
- ***Publicaciones y ataques públicos:** rumores, mensajes hirientes, fotos o videos humillantes publicados en redes sociales, blogs, foros, o enviados a través de la mensajería instantánea y del correo electrónico, y exclusión de grupos en línea, con los que denigrar a la persona implicada.*
- ***Ciberbullying mediante terceros**: uso de otras personas y mecanismos para ejercer el ciberacoso. Suplantación de identidad y creación de perfiles falsos en redes sociales y juegos en línea para enviar mensajes amenazantes o provocativos exponiendo a la víctima al escrutinio de terceros.*

¿Qué se debe hacer en caso de Ciberacoso?

En ningún caso se le quiere restar importancia a un ciberacoso, pero lo primero es averiguar el alcance real de cara a definir las medidas. No se debe actuar en la misma medida contra un alumno que se ría del tamaño de la nariz de un compañero (sin justificar ese comportamiento siempre reprobable), de un caso donde podría llegar a haber acoso sexual entre un adulto y un menor.

Para los casos más “leves” en los que se involucra a menores podría ser suficiente con contactar con el centro escolar (en caso de que se se produzca en el entorno escolar), contactar con los tutores legales del acosador e intentar solucionar el incidente de manera dialogada.

Para casos más graves es necesario presentar una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado o autoridades judiciales para iniciar una investigación, identificar al responsable y ponerlo a disposición de la Justicia. En este punto dado la volatibilidad de las pruebas es necesario contar con el apoyo de un perito informático que dirija la obtención de evidencias digitales para sustentar la denuncia apoyado por un fedatario público que otorgue veracidad a la prueba obtenida.

Sólo una correcta investigación y una obtención de pruebas consiguiendo la custodia de las mismas puede garantizar la validez de las mismas de cara a un procedimiento judicial. Si tiene cualquier pregunta respecto a este tema o referente a un caso de este tipo no dude en contactar con nosotros.

Autor: Carlos Pintos Teigeiro
Informática y Peritaje
http://www.informaticayperitaje.com