2.1 Uso indebido de las redes

Fuente: https://cutt.ly/dzQYi2l

Todos somos libres de divulgar nuestros datos como queramos, pero debemos de ser conscientes de que todo hecho trae consigo consecuencias y más aún a través de Internet ya que somos más vulnerables. No conocemos realmente a la persona que está al otro lado de la pantalla y por ello tenemos que andarnos con cautela, puesto que una persona con malas intenciones puede dañar nuestra imagen y reputación.

La inadecuada utilización de las redes sociales es una de las problemáticas que actualmente se están presentando en los jóvenes, quienes son los principales usuarios de estas y al ser menores de edad o no contar con la madurez necesaria pueden estar en peligro sin siquiera enterarse. Esta es una de las principales preocupaciones que tienen los educadores, padres de familia y personas allegadas a los jóvenes que no le dan un adecuado uso a las redes sociales o han sido víctimas de algún acontecimiento ligado a este problema y desean que no continúe ocurriendo.

Las redes sociales son un fenómeno inherente del ser humano, como se desprende del comentario de Hütt (2012): “Las relaciones interpersonales son parte de la esencia natural del hombre, y sin lugar a dudas esta dinámica es trasladada a las organizaciones, las cuales como entes vivos y simbióticos requieren y dependen de una interacción permanente entre sus integrantes” (p. 122). La forma en que nos relacionamos ha sido estudiada junto con la humanidad; actualmente las conocemos ligadas a las plataformas de las tecnologías de información y comunicación (TIC), sin embargo, este es su medio de transmisión más reciente. No obstante, para comprender las redes sociales en línea, debemos primero comprender qué es en sí una red social. En su artículo, Peyró (2015) dice:

> Como mecanismo de adaptación y supervivencia formamos parte de diferentes grupos, desde la familia a los amigos, en todos los ámbitos, académicos, profesionales, culturales, etc. De este modo, los seres humanos estamos inmersos de manera permanente en una red de relaciones, y establecemos conexiones con nuestros iguales pues como seres sociales necesitamos relacionarnos, tomar contacto con el otro. Formamos parte de redes, y en ellas definimos y son definidos nuestros roles, nuestras relaciones, y en base a estas, obtenemos y transmitimos información relevante para diversos ámbitos de nuestra vida. (p. 236)

Según Vanderhoven et al. (2014), los peligros de contenido se entienden como aquellos mensajes de odio y mensajes diversos, entre otros que podrían influenciar negativamente a nuestra niñez y juventud. En este rango se incluyen: acceso a pornografía, mensajes racistas, xenofóbicos, sectarios, entre otros. Los de contacto están ligados a todos los medios de comunicación que existen hoy en día a través de las TIC, dígase mensajerías SMS, mensajería instantánea, chats, redes sociales, entre otros, estos están ligados a ciberbulling, acoso sexual, riesgos de privacidad, donde los datos y fotos personales puedes ser sustraídos. El último, el comercial, se liga al uso indebido de la información y fotos personales, uso de los datos para hacer seguimiento del comportamiento de la niñez y la adolescencia.

Por ello debemos primero conocer bien los peligros a los que está expuesta nuestra niñez y adolescencia y, posteriormente, cómo podemos protegerla. Como menciona García- Maldonado, Joffre-Velázquez, Martínez-Salazar y LLanes Castillo (2011): “La participación de los padres es muy importante, pues muchos imponen reglas a sus hijos acerca del uso que deberían hacer de Internet, y, sin embargo, no son realmente conscientes de las amenazas que se encuentran en la red” (p. 123). Se puede tener leyes y sistemas educativos con mecanismos de vigilancia, pero son los padres y madres la primera barrera de protección de sus hijos e hijas. “Estas acciones deben fortalecerse con la participación de los padres de familia, para que sus hijos hagan un uso adecuado de las redes virtuales y de la tecnología” (Maya-Alvarado, TapiaQuintana citados por García-Maldonado et al., 2011, p. 124).

Entre las formas más comunes de delinquir por medio de las redes sociales, podemos destacar las siguientes:

a) **Ofensas contra el honor**: Se trata de manifestaciones ofensivas proferidas para dañar el honor de una persona determinada (o contra varias) en la red social del propio emisor o del destinatario, o publicadas en los comentarios de otros usuarios de dichas redes sociales. El honor, entendido como uno de los valores fundamentales para el desarrollo de la personalidad en una sociedad que, dependiendo de la magnitud de la ofensa, se ve dañado en muchos casos de forma irreversible, de las siguientes formas:

- **Injurias:** Son comunicaciones ofensivas dirigidas de forma directa contra una persona determinada o que le fueron expresadas a ésta dentro de un grupo del que forma parte o no (como Whatsapp); o una publicación en Instagram de una imagen con un texto ofensivo; o un comentario publicado en el perfil propio u otro de Twiter; o un comentario contra una persona determinada publicado al pie de una noticia en un medio de prensa digital. Una ofensa constitutiva de una injuria puede converger -a la misma vez- con la difamación, y con la calumnia, cuando se emite de forma tal que encuadra en las tres (o en dos) de esas formas y conforme a las reglas del concurso ideal.

- **Difamación:** Las ofensas se lanzan contra una persona (o varias) en un entorno público o -inclusive- restringido (como los perfiles de Facebook), o ante una diversidad de personas que comparten virtualmente (como un grupo de WhatsApp), y estas se lanzan con la intención de que sean leídas por una pluralidad de usuarios de las redes sociales para dañar el honor de la persona a la que se refieren. Hay quienes creen erradamente que publicándose hechos ciertos no se difama el honor de alguien, lo cual es totalmente errado porque aun con “verdades” se puede dañar el honor de una persona y más si se trata de hechos que forman parte de la vida privada. Por ejemplo, constituye una difamación cuando se difunde (por ejemplo en Facebook) la sentencia de un delito por el cual una persona fue condenada en el pasado y en un entorno grupal donde no se sabía nada de ello; o -por ejemplo- con la intención de dañar el honor de otro, publicar en un chat de WhatsApp de padres de familia de la escuela o colegio acerca de que a determinada persona le impusieron medidas de restricción por violencia intrafamiliar; o, también por ejemplo, se daña el honor cuando se difunden en redes sociales imágenes o vídeos relacionados con la vida íntima sexual de una persona, que pudieron haberse obtenido con autorización o no de la persona afectada, pero nunca para ser difundidos virtualmente.

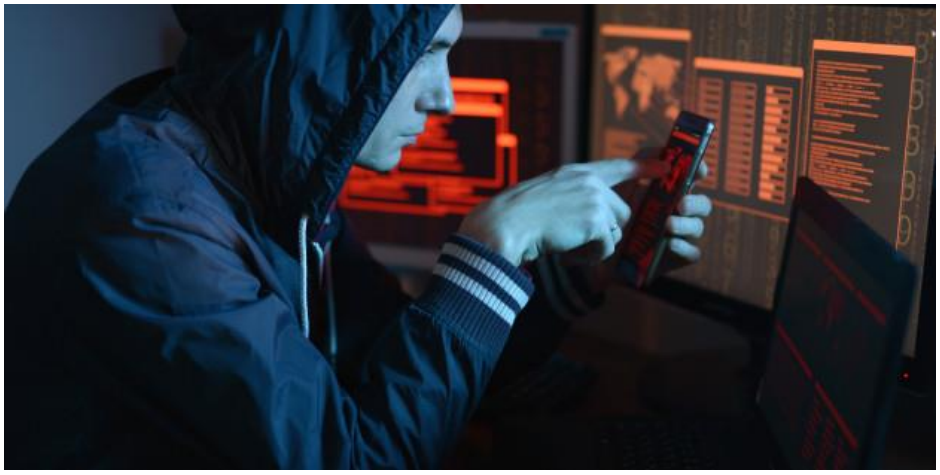
- **Calumnia:** Es la afirmación falsa -en un entorno virtual- de la comisión de un hecho delictivo. Con solo que a esa manifestación falsa se le dé el carácter de apariencia de delito es una calumnia, sin que necesariamente se haga una calificación legal precisa, ya que estas últimas solo son de dominio de los abogados (y ni siquiera de todos…). La intención de la ofensa es presentar al destinatario de la misma como una persona que delinque o que actúa al margen de la ley. Así por ejemplo hay expresiones que se emiten en las redes sociales como “amigo de lo ajeno”, “tocón”, “agresor de mujeres” y otros términos coloquiales, con los que se hace referencia a conductas tipificadas penalmente, aunque no se haga mención al propio nombre técnico-jurídico con el que está tipificado en la ley.

- **Difamación de personas jurídicas:** Las ofensas en las redes sociales van dirigidas contra personas jurídicas (sociedades, asociaciones deportivas, etc.), o contra los personeros de estas que forman parte de grupos colegiados internos (como la Junta Directiva), los que también gozan de una reputación a nivel social. La intención del ofensor es dañar la confianza o el crédito del que gozan públicamente. Hay comercios, despachos profesionales, equipos de fútbol, y otros, que figuran como personas jurídicas formalmente registrados como tales. Por ejemplo, es muy dado en las redes sociales la publicación de ofensas o graves cuestionamientos contra la Junta Directiva de equipos de fútbol o contra dirigentes deportivos en esa condición.

- **Ofensas a la memoria de un difunto:** Suele suceder que algunas personas atacan el honor de una persona que ya ha fallecido, con la intención de dañar la grata memoria que se tenga de esta a nivel social. Hay personas que, a pesar de su fallecimiento, perduran en el tiempo y en la memoria de las personas que las conocieron personalmente u oyeron hablar de ellas. Las redes sociales se convierten en un medio ideal para dañar el buen recuerdo de una persona difunta que, muchas veces, es celosamente protegido por familiares y amigos hasta por varias generaciones. Se trata de una persona (con nombre y apellido) que esté declarada fallecida, y no la gloria o la reputación de un apellido.

b) Coacción, extorsión o amenazas agravadas: Es muy frecuente que, por medio de las redes sociales, algunas veces por mucho tiempo, se coaccione a personas que son sometidas al acoso moral y psicológico de depredadores virtuales, sin que estén obligadas a soportarlo, y quienes son víctimas de la publicación de imágenes o de comentarios proferidos con la intención de intimidar a determinadas personas para que hagan o no hagan algo a lo que no están obligadas. Por ejemplo, es frecuente la coacción cuando se publican en las redes sociales (como en Facebook) mensajes indirectos, o algunas veces explícitos, que cuestionan la paternidad o la maternidad responsable de una persona con el propósito de presionarla a que realice determinados actos, como podría ser el pago de una pensión alimentaria mayor al que se le obligó en una sentencia.

La extorsión se da cuando se intimida de cualquier forma o se amenaza con la realización de una acción grave para obligar a otro a procurar un beneficio patrimonial para sí o para un tercero, cuya conducta se agrava cuando la conducta se realiza valiéndose de cualquier manipulación tecnológica; es decir, mediante mensajes privados que tienen algunas redes sociales como la mensajería del propio aparato celular o la de Messenger, Telegram o Instagram. Las amenazas graves suceden cuando se anuncia la realización de resultados más específicos que están determinados en la misma Ley (como la amenaza de muerte); también cuando se anuncia la publicación de vídeos o imágenes (en Facebook) amenazándose con su difusión a terceros por simple venganza; o cuando se anuncia la realización de un daño sobre una cosa o una lesión a una persona determinada.



Fuente: https://cutt.ly/szQYYRP

c) Estafas informáticas u otros fraudes: Es cada vez más usual que algunas personas, mediante la utilización de perfiles falsos, se hagan pasar en las redes sociales por determinadas personas (conocidas de las víctimas) para solicitar dinero mediante el ardid de una emergencia inexistente como afirmar -por ejemplo- que se encuentra en un aeropuerto del extranjero y que se quedó sin dinero, o que tiene una emergencia hospitalaria, con el propósito de que le transfieran dinero inmediato a una cuenta bancaria; o también sujetos que diseñan perfiles falsos en las redes sociales -con la apariencia de una entidad bancaria- para solicitar información privada que les permite el acceso a cuentas bancarias para defraudar de cualquier forma a personas o a empresas (pishing); o bien, cuando en una red social una agencia ofrece la venta de tiquetes aéreos o cruceros, y son contactados de esa forma para que giren pagos de dinero que realmente nunca se van a materializar en ningún viaje.

d) Modalidades de acoso: Hoy día abundan diferentes formas de acoso a personas que se ejecutan por medio de las redes sociales abiertamente, ya sea en el perfil del acosado/a o del acosador/a, mediante mensajes simbólicos o comentarios directos al pie de publicaciones o a través de mensajería privada (Messenger, WhatsApp o mensajes de texto), que da lugar a diferentes actos que podrían constituir delitos que se materializan por medio de sexting, acoso cibernético, ciberviolencia (ciberbullyng), ciber moobing, stalking y child-grooming. Estas acciones podrían dar lugar a delitos de coacción, amenazas u ofensas; o peor aún, desatar hechos más graves como suicidios y homicidios, todos originados en un acoso virtual.

e) Grabación y difusión indebida de imágenes: Se ha convertido en una práctica de jóvenes y adultos grabar vídeos o tomarse fotografías (cuyas imágenes se fijan sin autorización mediante “screenshots”) que podrían comprometer la reputación y la probidad de personas. Alguna tiene el fetiche de tomarse fotografías de sí mismas o de tomarle a otras desnudan, o de grabar vídeos íntimos de contenido sexual que, en manos de una persona autorizada o no, podrían ser difundidos en redes sociales en perjuicio de la víctima con el único propósito de hacer daño, comercio o, inclusive, utilizarse para una extorsión con la amenaza de su difusión viral en redes sociales.

Fuente: https://cutt.ly/kzQYKpZ

f) Corrupción de menores de edad: Las redes sociales son el caldo de cultivo para que pedófilos, pederastas y todo tipo de depredadores sexuales, contacten de manera encubierta (casi siempre mediante perfiles falsos para aparentar una edad menor de la que realmente tienen) a víctimas menores de edad con quienes entran hábilmente en confianza para sus propósitos sexuales, creyendo las víctimas que se trata de personas de su misma edad o similar. Así, mediante el contacto virtual, los corruptores logran envolver en sus tentáculos a menores de edad quienes ingenuamente caen en distintas solicitudes o favores que les solicitan con el propósito de satisfacer los instintos sexuales enfermizos de estos corruptores que pueden ser para su uso personal o para el negocio de difusión de pornografía infantil. Lamentablemente un buen número de menores de edad se corrompen no solo por ingenuidad, sino de manera consciente porque se encuentran en tal condición de vulnerabilidad (pobreza, baja autoestima, etc.) que los convierte en las víctimas ideales para este tipo de delitos, lo que es aprovechado por este tipo de personas para sus fines inescrupulosos.

2.1.1 Grooming

También conocido como ciberacoso sexual a menores a través de internet, teléfono o redes sociales. Para Arab y Díaz (2015), “es un conjunto de estrategias que una persona adulta desarrolla para ganar la confianza del/la [*sic*] joven a través de internet… adquiriendo control y poder sobre él/ella, con el fin último de abusar sexualmente de él/ella” (p. 10). Podemos definirlo como el conjunto de estrategias que un adulto usa para ganarse la confianza de una menor a través de Internet para obtener concesiones de índole sexual.

Según Peña (2014) esta fase es conocida como El Enganche, donde el agresor que ingresa al entorno digital manifiesta gran interés por contactar a un amplio número de niños, niñas y adolescentes que pueden terminar siendo un gran potencial para el abuso y la explotación sexual en el entorno virtual, pues no existen límites en la utilización de todo el sistema digital para producir delitos. Ver imagen 4.

Imagen 4. Ilustrativa del grooming
Fuente: https://www.madariaga.gob.ar/noticias/18803/hoy-es-el-dia-nacional-de-la-lucha-contra-el-grooming

El grooming se define como el acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor, incluyéndose en este desde el contacto físico hasta las relaciones virtuales y la obtención de pornografía infantil. Se caracteriza por:

Inicio de una relación: Hace referencia a la toma de contacto con el menor de edad para conocer sus gustos, preferencias y crear una relación con el objeto de alcanzar la confianza del posible afectado.

Inicio de una supuesta amistad. La fase de formación de una amistad incluye con frecuencia confesiones personales e íntimas entre el menor y el acosador. De esta forma se consolida la confianza obtenida del menor y se profundiza en información sobre su vida, sus gustos y sus costumbres.

Componente sexual. El objetivo final de este acercamiento es de carácter sexual. Con frecuencia incluye la descripción de términos específicamente sexuales y la petición a los menores de su participación en actos de naturaleza sexual, grabación de imágenes o toma de fotografías.

En el grooming se determinan, además, una serie de fases por las que el adulto consigue hacerse con la confianza del menor y consumar el abuso:

Contacto y acercamiento: el acosador contacta con el menor a través de diferentes servicios como puede ser mensajería instantánea, chat o redes sociales y habitualmente finge ser otro menor de edad similar, físico que le pueda resultar atractivo, similitud en sus gustos, etc

Sexo virtual: con la amistad conseguida, el acosador puede llegar a conseguir, que el menor le envíe alguna fotografía comprometida, logrando que encienda la webcam o que pose desnudo, total o parcialmente.

Ciberacoso: en el momento en el que posee alguna de estas imágenes o vídeos, incluso conversaciones que el menor puede considerar comprometidas, si el menor no accede a sus pretensiones, el acosador le amenaza con difundir esta información a través de diferentes medios

Abuso y agresiones sexuales: ante las amenazas del acosador el menor accede a sus exigencias, pudiendo llegar a contactar físicamente y mantener relaciones.

Los groomers pueden ser hombres o mujeres de cualquier edad o situación económica, que usan técnicas para ganarse a los niños y a sus familias, empiezan ofreciendo consejos y compresión, luegos les obsequian con regalos y finalmente los chantajean para obtener fotos comprometidas o quedar en persona. Pero además consiguen asustar y controlar tanto a la víctima que hace que esta se sienta avergonzada, culpable y no lo denuncie.

Por todo ello es necesario que los mayores controlen y supervisen el acceso de los menores a Internet, que concienciemos a los menores de los peligros que hay y les ofrezcamos nuestro cariño si tienen este problema, que les apoyemos y no les reprochemos lo ocurrido. Por otro lado, los niños no deben de tener miedo, deben contarlo y denunciar, pero para ello deben recopilar conversaciones, fotos o cualquier información del groomer.

La Ley 1273 de 2009 complementa el código penal y estructura un ambiente jurídico para la protección de la información y de los datos, con el cual se protege la integridad y seguridad de los sistemas que utilicen las tecnologías de la información y las comunicaciones, así como de quienes hacen uso de ellos. El primer capítulo de los dos en que está dividida la ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La Ley 1273 de 2009 carece de una penalización directa sobre el ciberacoso infantil.

La siguiente figura ilustra claramente cómo las conductas o patrones comportamentales de los agresores sexuales en el ciberespacio se transforman progresivamente hasta lograr involucrar a los menores de edad en actividades sexuales y obtener material ilícito suficiente para iniciar la fase de acoso sexual cibernético o ciberacoso sexual infantil, el cual está enfocado en la creación de un ambiente hostil que posee o poseerá efectos devastadores para el bienestar físico, mental o emocional de los niños, niñas, jóvenes y adolescentes (Bartrina, 2014).

Figura 1. Etapas y conductas asociadas al delito de Gromming
Fuente: Elaboración propia

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia junto con el Instituto Colombiano de Bienestar Familiar, el Foro de Generaciones Interactivas, la red PaPaz y la Policía de Infancia y Adolescencia en coordinación con el Centro Cibernético Policial, son las principales instituciones encargadas de proteger la integridad de los menores de edad contra el delito de Grooming en Colombia y sus agravantes. La línea virtual Te Protejo en Colombia funciona como principal vía de comunicación para denunciar a tiempo casos de explotación sexual comercial de niños, niñas y adolescentes, pornografía infantil, ciberacoso, intimidación escolar, contenidos inapropiados en la web, entre otros delitos, esto le ha permitido a la Dirección de Investigación Criminal Internacional o INTERPOL desarrollar estrategias innovadoras, programas contundentes y proyectos efectivos en pro de promover y cooperar a la investigación criminal y a la eliminación y bloqueo de varios sitios web con contenido ilícito (MinTic, 2017)

El delito de Grooming en Colombia constituye ordenes de carácter punitivo por la violación de datos personales (Artículo 269F) y la suplantación de sitios web para capturar datos personales (Artículo 269G), cuyo agravante o motivo legal para recargar la pena correspondiente a dichos 27 delitos tiene que ver con la vulneración a la integridad de los niños, niñas y adolescentes por la comisión de abuso sexual infantil o distribución de material con contenido sexual ilícito en el entorno virtual. La siguiente tabla explica con precisión las normas sustantivas y procesales que castigan no solo el hecho de cometer un delito informático donde muchos usuarios utilizan diferentes identidades para captar datos personales e información privada de los menores de edad, también penaliza, en conformidad con Artículo 20 (Derechos de Protección) del Código de Infancia y Adolescencia “la violación, la inducción, el estímulo y el constreñimiento a la prostitución; la explotación sexual, la pornografía y cualquier otra conducta que atente contra la libertad, integridad y formación sexuales de la persona menor de edad” (Congreso de la República, 2006).

2.1.2 Sexting.

Su nombre es un acrónimo de 'sex' o sexo y 'texting' o escribir mensajes. Consiste en enviar mensajes, fotos o vídeos de contenido erótico y sexual personal a través del móvil mediante aplicaciones de mensajería instantánea o redes sociales, correos electrónicos u otro tipo de herramienta de comunicación, ver imagen 5.

Estamos hablando del 'grooming' que consiste en establecer lazos de amistad con un niño o niña, de manera deliberada por parte de un adulto, para obtener satisfacción sexual mediante el envío de imágenes eróticas o pornográficas del menor, solicitando estas, o incluso como medio y preparación a un encuentro sexual posterior. Efectivamente, se refiere a la pederastia y supone un grave problema sobre la seguridad de los menores en Internet.

Imagen 5. Acoso en ambientes escolares
Fuente: https://www.pinterest.es/pin/420805158908401725/

Este peligro en las redes sociales surge de la necesidad de la persona menor de edad de
ser aceptada y avalada por sus pares o por intereses sentimentales. El sexting, por definición, se entiende como:

Práctica que consiste en compartir imágenes de tipo sexual, personal o de otros, por medio de teléfonos o internet. El riesgo, es que las imágenes sean publicadas y viralizadas sin permiso. Con ello la intimidad queda expuesta a la mirada pública. (Arab y Díaz, 2015, p. 10) Es una práctica común en la juventud, que da paso a otros peligros, como el acoso o la pornografía infantil.

Consiste en enviar contenidos de tipo sexual producidos generalmente por el remitente a otras personas a través de móviles, normalmente a su pareja o a amigos como si fuera un simple juego, pero este al final no acaba bien.

Algunas de las principales causas son:

- Noviazgo o coqueteo
- Presión de los amigos
- Impulsividad
- Lucimiento
- Venganza
- La confianza en la discreción
- Creer que una imagen en un móvil está segura

Algunos expertos y estudios afirman que la raíz del problema es el contexto natural en el que crecemos, con un gran culto al cuerpo y a las celebridades que hacen que los imitemos. Es decir, si un famoso hace sexting, y esto se transmite a los medios contribuye a normalizar la situación lo que hace que no lo veamos mal y lo hagamos.

Para poder entenderlo y abordarlo con más exactitud se deben tener en cuenta ciertos factores claves que influyen en su descripción, así como en el daño potencial del protagonista:

• **El origen de la imagen:** puede ser de producción propia, de producción ajena, pero con consentimiento del protagonista y, robado.

• **El contenido de la imagen:** esto se refiere a la dificultad de determinar la carga sexual de algunas imágenes y poder definirla como atrevida, erótica, pornográfica…

• **La identificabilidad:** alude a la posibilidad de identificar o no al protagonista de la imagen.

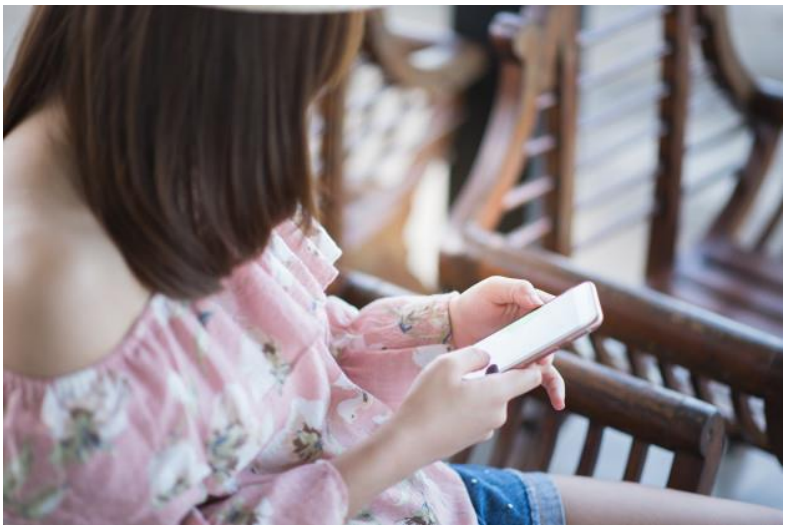
• **La edad del protagonista:** existen dificultades en la determinación de la mayoría o minoría de edad en el protagonista de la imagen por el anonimato.

Existen numerosos aspectos que agravan la práctica del sexting entre los adolescentes. De entre ellos podemos destacar:

1. Inconsciencia de riesgo potencial: “Ellos no sienten el peligro de las nuevas tecnologías porque nacieron con ellas y se imitan a través de éstas” En este sentido, la culpa no radica en los recursos que ofrece Internet, sino la propia percepción de los adolescentes, los cuales: “no perciben la diferencia entre lo que es público y lo que es privado”. (De Domini, 2009; citado por Menjívar, 2010).
2. Brecha generacional: hace alusión a la falta de comprensión de la generación de migrantes tecnológicos de los usos y nuevos códigos de socialización y vivencia de la sexualidad de los nativos tecnológicos (Menjívar, 2010).
3. Sexualidad precoz de la infancia: este concepto se refiere a la tendencia que se está dando en los últimos años de adelantar la adolescencia a edades cada vez más tempranas, manifestándose sobre todo en las niñas e implicando el desarrollo de las características propias de la edad, entre ellas la definición sexual. (Pérez et al., 2011).
4. Inmediatez de las comunicaciones: el acceso a las nuevas tecnologías brinda cada día una mayor disponibilidad, facilidad, portabilidad y economía, lo que implica que los impulsos pueden hacerse realidad sin posibilidad de vuelta atrás.

El Sexting supone la pérdida de privacidad, ya que los contenidos de temática sexual que una persona genera y envía a otra y otras, pueden acabar en manos no deseadas, perdiendo el control sobre su difusión. Uno de los problemas principales que conlleva el sexting, además de la degradación personal y la pérdida de privacidad, es la aparición de ciertos comportamientos delictivos como el grooming, el ciberbullying y la sextorsión

Según el Código Penal, cuando hay constreñimiento ilegal la condena por el delito puede oscilar entre 16 a 32 meses de prisión. Cuando aparece la extorsión, amenazas de usar la violencia o intimidar a cambio de dinero u otro ligado a un posible perjuicio patrimonial, la pena aumenta a unos 16 a 24 años de prisión.



Fuente: https://acortar.link/bGczY

2.1.3 Ciberbullying

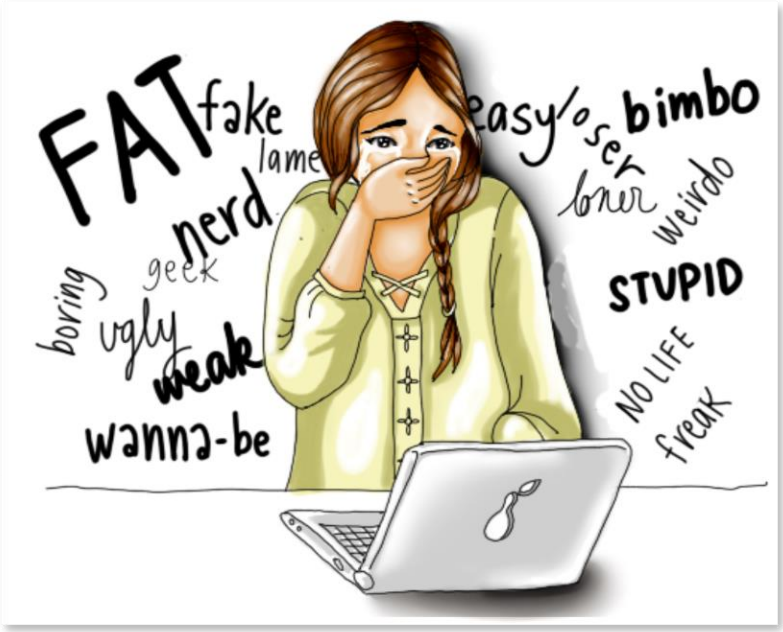


Imagen 6. ciberbullying
Fuente http://www.educatolerancia.com/siete-diez-victimas-ciberbullying-chicas/

El ciberbullying (o ciberacoso escolar), que se puede definir como una forma de ataque virtual que perturba la integridad emocional de las personas, especialmente de quienes se encuentran, en gran medida, entre las edades de 10 a 20 años. Cabe señalar que este acoso virtual es propio de un contexto neoliberal, en el que la individualidad es una realidad cada vez más presente y que lleva a nuestra sociedad al egoísmo, lo que produce desesperanza en preadolescentes y adolescentes para encontrar un escape. Así, entonces, el ciberbullying está presente en las redes sociales para escuchar y atacar, con el objeto de colmar el vacío afectivo y la carencia de amor.

Consiste en el uso de medios telemáticos para ejercer el acoso psicológico entre iguales. Es decir, cuando un menor está atormentado y hostigado por otro a través de Internet.

Se da en los siguientes casos:

Colgar en internet una foto comprometida o datos delicados que avergüenzan a la víctima.

Crear perfiles falsos con los datos de la víctima donde se escriban a modo de confesiones en primera persona algunos acontecimientos personales.

Enviar SMS o mensajes amenazantes, perseguir y acechar a la víctima en los lugares que normalmente visita, todo vía Internet.

Hacer correr rumores en lo que la víctima tenga un supuesto comportamiento desleal, haciendo que sean otros quienes emprenden con su propia forma represalias.

Usurpar su clave de correo electrónico, leer sus mensajes y por lo tanto violar su identidad.

La característica principal de este tipo de ataque virtual se manifiesta en el hostigamiento, los insultos, la infamación y otros más, que van quebrantando la dignidad de la persona y pueden ocasionar, posteriormente, trastornos de la salud mental. Para analizar este problema, es necesario mencionar sus causas y una de ellas es su permanencia en las redes sociales, las cuales se entienden como “la existencia de las redes humanas determinadas por las tecnologías y la ciencia en las que el ser se ha constituido como un número o como un código de identificación” (Becker, 1977, p. 82). Se ve entonces, cómo, sin ninguna oposición, ellos — los jóvenes que viven su preadolescencia y adolescencia aceptan formar parte del consumismo que traen las tecnologías, las cuales no hacen distinción de clase, raza, sexo o condición humana.

Fuente: https://acortar.link/0Kaih

¿Cómo se manifiesta el ciberbullying?

Las formas que adopta son muy variadas y sólo se encuentran limitadas por la pericia tecnológica y la imaginación de los menores acosadores, lo cual es poco esperanzador. Algunos ejemplos concretos podrían ser los siguientes:

- Colgar en Internet una imagen comprometida (real o efectuada mediante fotomontajes) datos delicados, cosas que pueden perjudicar o avergonzar a la víctima y darlo a conocer en su entorno de relaciones.
- Dar de alta, con foto incluida, a la víctima en un web donde se trata de votar a la persona más fea, a la menos inteligente… y cargarle de *puntos* o *votos* para que aparezca en los primeros lugares.
- Crear un perfil o espacio falso en nombre de la víctima, en redes sociales o foros, donde se escriban a modo de confesiones en primera persona determinados acontecimientos personales, demandas explícitas de contactos sexuales…
- Dejar comentarios ofensivos en foros o participar agresivamente en chats haciéndose pasar por la víctima de manera que las reacciones vayan posteriormente dirigidas a quien ha sufrido la usurpación de personalidad.
- Dando de alta la dirección de correo electrónico en determinados sitios para que luego sea víctima de spam, de contactos con desconocidos…

- Usurpar su clave de correo electrónico para, además de cambiarla de forma que su legítimo propietario no lo pueda consultar, leer los mensajes que a su buzón le llegan violando su intimidad.
- Provocar a la víctima en servicios web que cuentan con una persona responsable de vigilar o moderar lo que allí pasa (chats, juegos online, comunidades virtuales…) para conseguir una reacción violenta que, una vez denunciada o evidenciada, le suponga la exclusión de quien realmente venía siendo la víctima.
- Hacer circular rumores en los cuales a la víctima se le suponga un comportamiento reprochable, ofensivo o desleal, de forma que sean otros quienes, sin poner en duda lo que leen, ejerzan sus propias formas de represalia o acoso.
- Enviar menajes amenazantes por e-mail o SMS, perseguir y acechar a la víctima en los lugares de Internet en los se relaciona de manera habitual provocándole una sensación de completo agobio.

Consejos Generales

Tan pronto como tu hijo comience a usar internet es importante que le expliques cuáles son tus expectativas con respecto a su comportamiento. Al actuar de forma responsable y respetuosa, podrán disfrutar su tiempo en línea y disfrutar de lo mejor de internet y evadir en gran medida el ciberbullying y contenido inapropiado. Algunos consejos básicos que le puedes decir a tu hijo son:

Comunícate de forma apropiada. Usa el lenguaje adecuado para la ocasión. Probablemente no le escribas de la misma forma a tu maestro que a tus amigos. ¡Y recuerda que usar solo mayúsculas significa que estás gritando, así que no lo hagas!

Mantén privadas las cosas privadas. No compartas información como contraseñas, la dirección de tu casa, imágenes inapropiadas y chismes.

Respeta a los demás. Sé cortés y si no estás de acuerdo con algo, dilo de forma amable.

No mientas, robes, ni hagas trampa. No trates de engañar a otros, recuerda darle crédito a quien lo merece y, aunque es fácil copiar el trabajo de otro, no descargues nada sin permiso ni uses códigos para hacer trampa en juegos.

Apoya a quien lo necesite. Si alguien que conoces está siendo víctima de ciberbullying, ponte de su lado. A ti te gustaría que esa persona hiciera lo mismo por ti.

Reporta malos comportamientos. La internet es una comunidad gigante y es imposible que todo sea perfecto. Usa las herramientas de las redes para reportar contenido inapropiado.

Sigue las reglas de tu familia. Si tus padres te dicen que evites ciertos sitios web o que dejes de enviar mensajes de textos después de cierta hora, escúchalos. Mientras más responsable seas, más privilegios tendrás.

Piensa antes de publicar, enviar mensajes y compartir. Considera cómo tú y los demás se pueden sentir luego de que publiques algo. No siempre es fácil retirar lo dicho en línea y lo que hagas allí puede quedar registrado por mucho tiempo.

2.1.4 Phishing

Imagen 7. Pescando en la red
Fuente https://www.osi.es/es/banca-electronica

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o “suplanta su identidad”) a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.

El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude en las telecomunicaciones que emplea trucos de ingeniería social para obtener datos privados de sus víctimas.

Un ataque de phishing tiene tres componentes:

El ataque se realiza mediante comunicaciones electrónicas, como un correo electrónico o una llamada de teléfono.

El atacante se hace pasar por una persona u organización de confianza.

El objetivo es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito

¿Qué características tienen en común los correos de phishing?

Los mensajes suplantadores utilizan todo tipo de argumentos ingeniosos relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar sus datos personales. Entre las excusas frecuentes nos encontramos con:

Problemas de carácter técnico
Recientes detecciones de fraude y urgente incremento del nivel de seguridad.
Nuevas recomendaciones de seguridad para prevención del fraude.
Cambios en la política de seguridad de la entidad.
Promoción de nuevos productos.
Premios, regalos o ingresos económicos inesperados.
Accesos o usos anómalos a tu cuenta.
Inminente desactivación del servicio.
Falsas ofertas de empleo.

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

1. Bancos y cajas

Excusas utilizadas para engañar al usuario: cambio en la normativa del banco, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, bloqueo de la cuenta por motivos de seguridad, etc.
Objetivo: robar números de tarjetas de crédito, tarjetas de coordenadas, PIN secreto, etc.

2. Pasarelas de pago online (PayPal, Mastercard, Visa, etc.)

Excusas utilizadas para engañar al usuario: cambio en la normativa del servicio, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, etc.
Objetivo: al igual que en el caso del phishing anterior, principalmente robar datos bancarios

3. Redes sociales (Facebook, Twitter, Tuenti, Instagram, LinkedIn, etc.)

Excusas utilizadas para engañar al usuario: alguien te ha enviado un mensaje privado, se han detectado conexiones extrañas en la cuenta, por motivos de seguridad es necesario que se cambien las claves, etc.
Objetivo: robar cuentas de usuarios, obtener sus datos privados y suplantar su identidad.

4. Páginas de compra/venta y subastas (Amazon, eBay, etc.)

Excusas utilizadas para engañar al usuario: problemas en la cuenta del usuario, detectados movimientos sospechosos, actualización de las condiciones del uso del servicio, etc.
Objetivo: robar cuentas de usuarios y estafar económicamente al usuario

5. Juegos online

Excusas utilizadas para engañar al usuario: fallos de seguridad en la plataforma del juego, problemas en la cuenta del usuario.
Objetivo: robar cuentas, datos privados, bancarios y suplantar la identidad de los usuarios.

3. Redes sociales (Facebook, Twitter, Tuenti, Instagram, LinkedIn, etc.)

Excusas utilizadas para engañar al usuario: alguien te ha enviado un mensaje privado, se han detectado conexiones extrañas en la cuenta, por motivos de seguridad es necesario que se cambien las claves, etc.
Objetivo: robar cuentas de usuarios, obtener sus datos privados y suplantar su identidad.

4. Páginas de compra/venta y subastas (Amazon, eBay, etc.)

Excusas utilizadas para engañar al usuario: problemas en la cuenta del usuario, detectados movimientos sospechosos, actualización de las condiciones del uso del servicio, etc.
Objetivo: robar cuentas de usuarios y estafar económicamente al usuario

5. Juegos online

Excusas utilizadas para engañar al usuario: fallos de seguridad en la plataforma del juego, problemas en la cuenta del usuario.
Objetivo: robar cuentas, datos privados, bancarios y suplantar la identidad de los usuarios.

6. Soporte técnico y de ayuda (helpdesk) de empresas y servicios (Outlook, Yahoo!, Apple, Gmail, etc.)

Excusas utilizadas para engañar al usuario: confirmación de la cuenta de usuario, eliminación de cuentas inactivas, detectada actividad sospechosa en la cuenta, se ha superado el límite de capacidad de la cuenta, etc.
Objetivo: robar cuentas y datos privados de los usuarios.

7. Servicios de almacenamiento en la nube (Google Drive, Dropbox, etc.)

Excusas utilizadas para engañar al usuario:
Objetivo: Conseguir cuentas de distintos servicios de usuarios, obtener información privada.

8. Phishing a servicios o empresas públicas:

Excusas utilizadas para engañar al usuario: información sobre una notificación, una multa,
Objetivo: infectar el ordenador, robar datos privados, bancarios y estafar económicamente al usuario.

9. Phishing a servicios de mensajería

Excusas utilizadas para engañar al usuario: el paquete enviado no ha podido ser entregado, tienes un paquete esperando, información sobre el seguimiento de un pedido, etc.
Objetivo: infectar ordenadores, robar datos privados y bancarios de los usuarios.

10. Falsas ofertas de empleo

Excusas utilizadas para engañar al usuario: puestos de trabajo.
Objetivo: robar datos privados que pueden ser utilizados posteriormente con distintos fines fraudulentos.
.

Concejos para evitar ser víctima de phishing:

Sé precavido ante los correos que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.

Sospecha si hay errores gramaticales en el texto, pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.

Si recibes comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”, es un indicio que te debe poner en alerta.

Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.

Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta, y que ésta corresponda con la URL del servicio legítimo.

Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.

Aplica la ecuación: solicitud de datos bancarios + datos personales = fraude

2.2 Legislación del comportamiento digital (ley regulatoria del comportamiento en la web)

El Internet se desarrolla a una velocidad vertiginosa, que lo lleva siempre un paso adelante del derecho. Es preciso que el derecho analice las nuevas realidades tecnológicas y los regule cuando sea necesario para proteger los derechos de las personas, en forma flexible que no limite los avances en la materia.

La necesidad de preparar al sector de tecnologías de la información y las comunicaciones de Colombia para hacer frente a los desafíos que trae consigo el desarrollo de la convergencia tecnológica, institucional y de mercados, implicaba plantear un nuevo equilibrio entre la promoción del desarrollo competitivo del sector y el cumplimiento de los fines sociales de mayor cobertura y acceso de los ciudadanos, empresas e instituciones públicas a las TIC, derivados de la naturaleza de servicio público que ostentan las telecomunicaciones.

El Internet se desarrolla a una velocidad vertiginosa, que lo lleva siempre un paso adelante del derecho. Es preciso que el derecho analice las nuevas realidades tecnológicas y los regule cuando sea necesario para proteger los derechos de las personas, en forma flexible que no limite los avances en la materia.

La necesidad de preparar al sector de tecnologías de la información y las comunicaciones de Colombia para hacer frente a los desafíos que trae consigo el desarrollo de la convergencia tecnológica, institucional y de mercados, implicaba plantear un nuevo equilibrio entre la promoción del desarrollo competitivo del sector y el cumplimiento de los fines sociales de mayor cobertura y acceso de los ciudadanos, empresas e instituciones públicas a las TIC, derivados de la naturaleza de servicio público que ostentan las telecomunicaciones.

Colombia todavía no dispone de estadísticas sistemáticas sobre prácticas riesgosas en las redes de los menores de edad, en particular, y de los ciudadanos en general. No obstante, el conjunto de las obligaciones legales del Estado y la sociedad con los menores de edad, las experiencias nacionales documentadas por los medios de comunicación, y la experiencia internacional, conforman un caso que, en conjunto, motivan la adopción de una política de uso responsable de Internet y otras TIC (CID, 2010b).

En cuanto a las obligaciones constitucionales y legales, según la Constitución Nacional de Colombia, “Los servicios públicos son inherentes a la finalidad social del Estado. Es deber del Estado asegurar su prestación eficiente a todos los habitantes del territorio nacional” (Art. 365). Por su parte, el Código de Infancia y Adolescencia (Ley 1098 de 2006) señala como una responsabilidad de los medios de comunicación “abstenerse de realizar transmisiones o publicaciones que atenten contra la integridad moral, psíquica o física de los menores, que inciten a la violencia, que hagan apología de hechos delictivos o contravenciones, o que contengan descripciones morbosas o pornográficas” (Artículo 47). La norma establece también que “los niños, las niñas y los adolescentes tienen derecho a la intimidad personal, mediante la protección contra toda injerencia arbitraria o ilegal en su vida privada, la de su familia, domicilio y correspondencia. Así mismo, serán protegidos contra toda conducta, acción o circunstancia que afecte su dignidad” (Artículo 33). Finalmente, la Ley en referencia obliga a la adopción de franjas horarias de contenidos en televisión, infantiles y juveniles (Artículo 49), medida cuya efectividad se reducirá hacia el futuro cercano como regulador del uso de contenidos inapropiados para los menores de edad, en tanto los horarios de consumo de contenidos por Internet, incluida la televisión en línea, los define el usuario y no el generador de contenidos. El consecuente cambio tecnológico obliga a la adopción de herramientas de protección diferentes, como los programas de protección parental mencionados adelante.

El Código Penal colombiano (Ley 599 de 2000) no tipificaba los delitos cometidos a través de la computadora, cuando eran sancionados las leyes no existían y se trataban como la protección de un bien jurídicos tradicional en la correspondiente rama del derecho penal. Sin embargo, este ha sido objeto de reformas, para poder configurar los delitos informáticos. Como la ley 527 de 1999, que enmarca el uso de datos, del comercio electrónico y sobre las firmas digitales, o la ley 1266 del año 2008, que contiene y regula las disposiciones sobre el hábeas data y manejo de información sobre datos personales; aun así, estas leyes dejaban vacíos jurídicos para el uso inapropiado de la información, pero fueron la base para ley 1273 de 2009.

La apropiación de información confidencial es un acto ilegal, esta información obtenida ilegalmente podría estar almacenada en una computadora, en un medio magnético, en un celular, en un correo electrónico hasta en una USB. Este delito informático es castigado en Colombia Ley 1273 de 2009 denomina “De la Protección de la información y de los datos"·, se incorporan nuevas figuras delictivas en respuesta a la criminalidad informática con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes. Unos de los aspectos que logra fijar esta ley es la explotación de pornografía infantil, entonces en el 2001 se promulga en Colombia la Ley 679 que trata del estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad.

Según López. P (15 de febrero, 2018). Aunque no lo crea, cualquier tipo de intento de fraude, como el phishing o el robo de datos de páginas web inseguras, son los delitos informáticos que más se cometen en Colombia, seguido de la pornografía infantil que, en los últimos meses, se ha llevado toda la atención por el caso del 'Lobo Feroz'. Además "Entre 2016, 2017 y lo que va de 2018, hemos recibido 31.428 denuncias de todo tipo: abuso a un sistema informático, transferencia de datos no compartidos, entre otros": Wilson Pardo, subdirector de la Dijín.

De ahí la importancia de conocer el contexto y las consecuencias de los delitos informáticos y la normatividad aplicable en nuestro medio, para orientar posibles respuestas o formas de prevención y tratamiento. Ése es el sentido de la Ley 1273 de 2009, expedida en Colombia sobre delitos informáticos. En ella se hace una revisión de los delitos que atentan contra las principales características de calidad, de la información que, en últimas, son condiciones de seguridad (confidencialidad, integridad, disponibilidad) y lo que legalmente puede esperar el cliente de las organizaciones en las cuales ha depositado su confianza. Ver imagen 8.

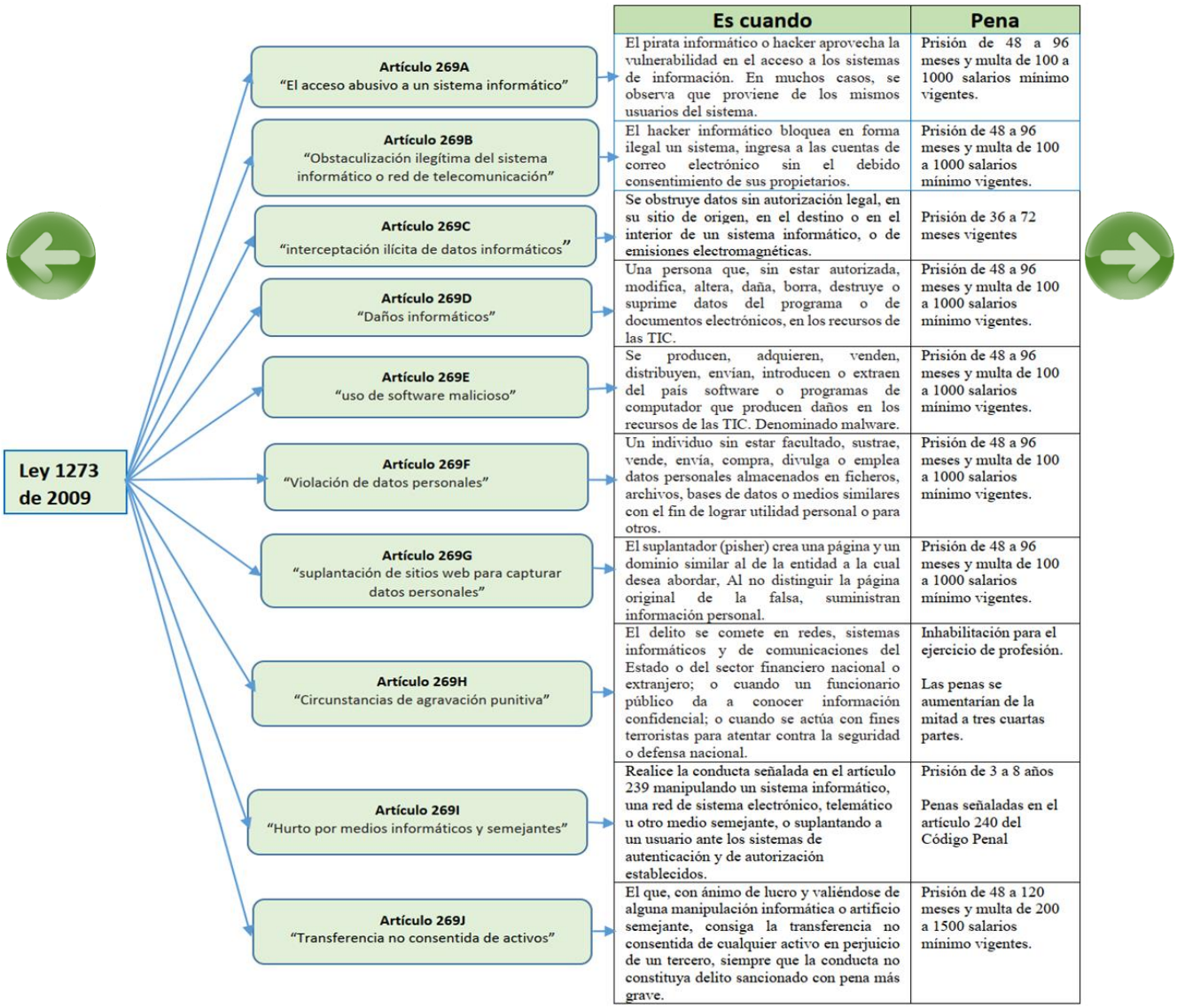
Concepciones sobre delito informático, complementarias todas, referidas por Suárez-Sánchez (2009), señalan un foco común con elementos distintos en su formalidad, mas no en su esencia:

- La especificidad del delito informático le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial (Choclán-Montalvo, 1997).

- La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software (Davara-Rodríguez, 2007).

- Podría ser delito informático todo comportamiento criminal en el que aparezca involucrado un ordenador; de este modo, casi cualquier delito con esta peculiaridad podría ser, eventualmente delito informático (Aldama-Baquedano, 1993).

- Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos (Gómez-Perals, 1994).



Es cuando	Pena
El pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información. En muchos casos, se observa que proviene de los mismos usuarios del sistema.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
El hacker informático bloquea en forma ilegal un sistema, ingresa a las cuentas de correo electrónico sin el debido consentimiento de sus propietarios.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
Se obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas.	Prisión de 36 a 72 meses vigentes
Una persona que, sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
Se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC. Denominado malware.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
Un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
El suplantador (pisher) crea una página y un dominio similar al de la entidad a la cual desea abordar, Al no distinguir la página original de la falsa, suministran información personal.	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimo vigentes.
El delito se comete en redes, sistemas informáticos y de comunicaciones del Estado o del sector financiero nacional o extranjero; o cuando un funcionario público da a conocer información confidencial; o cuando se actúa con fines terroristas para atentar contra la seguridad o defensa nacional.	Inhabilitación para el ejercicio de profesión. Las penas se aumentarían de la mitad a tres cuartas partes.
Realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.	Prisión de 3 a 8 años Penas señaladas en el artículo 240 del Código Penal
El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.	Prisión de 48 a 120 meses y multa de 200 a 1500 salarios mínimo vigentes.

Imagen 8. Ley contra fraudes electrónico
Fuente: autor

2.3 Mecanismos o estrategias para cuidar nuestra integridad en la web

Los diez comportamientos digitales son los siguientes:

1. Respeto: Utilizo las TIC respetando a los otros, respetándome y haciéndome respetar.

- Cuando utilizo las TIC me respeto y respeto a los demás siendo consciente de que todos somos personas dignas.
- Conozco que la injuria, la calumnia y la difamación son un delito o agravio contra el honor y el buen nombre de las personas.
- Sé que el ultraje de obra o palabra, divulgado a través de ambientes tecnológicos pueden lesionar e irrespetar los derechos, la intimidad y la dignidad de una persona u organización.

2. Libertad: Ejerzo mi derecho a la libertad y respeto la de los demás.

- Entiendo la libertad como la posibilidad de hacer lo que no daña a otro.
- Tengo la opción de decidir mi participación en cualquier actividad que me ofrezcan los ambientes tecnológicos y de hacer respetar mi decisión respetando siempre la de los demás.

3. Identidad: Hago uso de mi identidad de manera segura en mi interacción con los demás en ambientes tecnológicos.

4. Integridad: Protejo mi integridad y seguridad personal y la de los demás.

5. Intimidad: Soy responsable con mi intimidad y la de los demás.

6. Autonomía: Utilizo las TIC para libre desarrollo de mi personalidad y mi autonomía y
a través de ella reconozco y hago respetar mis creencias y pensamientos y los de los demás.

7. Calidad de vida: Utilizo las TIC para mejorar mi calidad de vida, asegurandome de procurar un ambiente sano y pacífico.

8. Cuidado y acompañamiento: Soy consciente de que los menores de edad requieren especial cuidado y acompañamiento en el uso de las TIC.

9. Respeto por la ley: NO utilizo las TIC para promover, consultar, comprar, compartir, actividades relacionadas con la explotación de menores, pornografía infantil, prostitución infantil, trata de conductas autodestructivas, organizaciones y/o actividades al margen de la ley o cualquier otra conducta que atente contra los derechos humanos.

10. Derechos de autor: Respeto los derechos de autor.