

CIBERACOSO EN MÉXICO, UNA FORMA DE CIBERCRIMINALIDAD Y VIOLENCIA DIGITAL

Cyberbullying in Mexico, a form of cybercrime and digital violence

Karla Karina SÁNCHEZ VILLA¹

SUMARIO. I. Introducción. II. Internet, nuevas tecnologías, redes sociales y ciberacoso. III. Ciberacoso como violencia digital en México. IV. La tipificación del ciberacoso en México. V. Conclusión. VI. Referencias.

Resumen. La violencia digital en México se manifiesta como un evento antijurídico en Internet y las redes sociales, representando un desafío para la sociedad al exponer a los usuarios a diversos riesgos, incluido el delito de ciberacoso, que afecta bienes jurídicos tutelados. Este trabajo de investigación aborda la problemática actual que enfrenta el Estado mexicano en relación con el ciberacoso. Explora cómo la influencia de Internet y las redes sociales desempeñan un papel crucial en la comisión de este delito, examina la forma en que se lleva a cabo, las repercusiones para la víctima y las modalidades conocidas como *Cyberbullying*, *Grooming* y *Sexting*. Además, analiza los índices de ciberacoso en México a

¹ Licenciada en Derecho por la Facultad de Derecho Culiacán de la Universidad Autónoma de Sinaloa y Maestra en Ciencias del Derecho en la Unidad Estudios de Posgrados de la Facultad de Derecho Culiacán de la Universidad Autónoma de Sinaloa. Participe en el panel sobre el “Día internacional de las víctimas de Desaparición forzada” el 30 de agosto de 2021 realizado por el H. Congreso del Estado de Sinaloa y la Universidad Autónoma del Estado de Sinaloa.

través del estudio de campo realizado por el Instituto Nacional de Estadística y Geografía, denominado "Modulo sobre Ciberacoso (MOCIBA) 2021". Por último, se examina la legislación actual en el Código Penal Federal con respecto a la conducta antijurídica del ciberacoso.

Palabras claves: Violencia digital, Ciberacoso, Cibercriminalidad, Bienes jurídicos tutelados, Internet.

Abstract. Digital violence in Mexico manifests as an unlawful event on the Internet and social media, posing a challenge to society by exposing users to various risks, including the crime of cyberbullying, which affects protected legal interests. This research addresses the current issue facing the Mexican state regarding cyberbullying. It explores how the influence of the Internet and social media plays a crucial role in the commission of this crime, examines how it is carried out, the repercussions for the victim, and the known modalities such as Cyberbullying, Grooming, and Sexting. Additionally, it analyzes cyberbullying rates in Mexico through the field study conducted by the National Institute of Statistics and Geography, known as the "Module on Cyberbullying (MOCIBA) 2021". Finally, it examines the current legislation in the Federal Penal Code regarding the unlawful conduct of cyberbullying.

Keywords: Digital violence, Cyberbullying, Cybercrime, Protected legal interests, Internet.

I. Introducción

En la actualidad, la mayoría de las interacciones sociales tienen lugar a través de dispositivos electrónicos, utilizando Internet y las redes sociales como herramientas de comunicación. Millones de personas se conectan para interactuar en todo el mundo. Sin embargo, estos medios también se utilizan para causar daño, siendo el ciberacoso una forma de violencia digital que se manifiesta a través de amenazas virtuales. Este tipo de cibercriminalidad está en aumento en México, y es crucial contar con legislación clara, precisa y aplicable para abordar estas conductas antijurídicas.

II. Internet, nuevas tecnologías, redes sociales y ciberacoso

En la sociedad contemporánea, Internet se ha convertido en un fenómeno global que conecta a millones de personas en todo el mundo. Esta red, conocida como la "Red de redes", ha

evolucionado en pocas décadas para convertirse en una herramienta indispensable para llevar a cabo diversas tareas. Complementada por una variedad de dispositivos electrónicos, como computadoras, laptops, iPads, tablets y smartphones, las cuales facilitan considerablemente la ejecución de estas actividades. Internet y los dispositivos electrónicos forman parte integral de nuestra vida cotidiana, utilizándose en entornos como la escuela, la oficina, el trabajo, el gobierno y el hogar. Además, se han integrado de manera significativa como una forma placentera de pasar el tiempo, navegando por la Web y participando en las redes sociales.

La era digital ha llegado para quedarse, y las tecnologías han sido ampliamente aceptadas, convirtiéndose en elementos fundamentales de la vida moderna. Cada día, Internet y los dispositivos electrónicos experimentan constantes actualizaciones. Por ende, es imperativo que las personas no se queden rezagadas; deben avanzar al mismo ritmo para mantenerse al día con la tecnología informática y seguir beneficiándose de la amplia gama de servicios que ofrece.

Como nos dice Miró Llinares, las relaciones que se desarrollan a base del impacto y crecimiento de la era digital conllevan al surgimiento de la denominada Sociedad de la información, un entorno virtual donde todas las personas usuarias de Internet y los medios informáticos están interconectadas en ese mismo ambiente, formando una conexión entrelazada unas con otras, con el propósito principal de compartir, desarrollar, producir y difundir información mediante la Web y las redes sociales. Internet se ha convertido en un medio universal para las relaciones interpersonales y, debido a sus propios objetivos y características, se nutre de información. Todas las relaciones, ya sean personales o comerciales, que se desarrollan en la red son esencialmente transferencias de información².

Es tanto el auge que ha tenido la Red en México que actualmente el acceso a Internet se ha convertido en un Derecho Humano desde el 11 de junio de 2013, consagrado en la Constitución Política de los Estados Unidos Mexicanos en el Título primero denominado De los Derechos Humanos y sus garantías, en el artículo 6º párrafo tercero donde se establece:

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones,

² Miró Llinares, Fernando, *Internet y delitos contra la propiedad intelectual*, España, Edición Fundación Autor, 2005, p. 33.

incluido el de banda ancha e Internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.

Dicho de esta manera, con el precepto legal anteriormente citado, el Estado mexicano salvaguarda y protege el Derecho humano de acceso a Internet en México como un Derecho fundamental, dándole firmeza jurídica y sustento legal para que la Red se encuentre al alcance de todos los usuarios, y con dicha herramienta, puedan compartir su manifestación o expresión de ideas sin distinción de su condición social, económica o de género; asimismo, impedir o prohibir el acceso a Internet será considerado como una violación a los Derechos humanos.

Sin embargo, surgen las siguientes inquietudes: ¿Es completamente seguro navegar por la red? ¿No hay riesgos en la web? Es así como el Estado mexicano también debe abordar estas preguntas y esforzarse por garantizar que Internet sea segura, proporcionando un entorno de paz y confianza para los internautas.

Las redes de Internet han creado posibilidades infinitas para que las personas trabajen, se comuniquen, aprendan, compren, vendan, jueguen, interactúen con otras personas de otras partes del mundo. Esas posibilidades provienen de la apertura de las redes especialmente de Internet, el cual está disponible prácticamente para todas las personas y para todos los tipos de usos. Sin embargo, la gran apertura que hace que Internet sea tan valioso también hace que sea un conducto de muchos tipos de amenazas³.

Como ya hemos mencionado anteriormente, los numerosos beneficios que nos brinda Internet son incuestionables, ya que facilita comunicaciones más rápidas. Sin embargo, es crucial enfatizar un punto muy importante: los riesgos asociados con Internet. Como usuarios de la web, no podemos pasar por alto estos riesgos, ya que estamos vulnerables a sufrir ataques que podrían afectar nuestra esfera jurídica.

El peligro que se cometan delitos a través de Internet es latente, pues en el ciberespacio se maneja todo tipo de información; pública, privada, comercial, defensa nacional e inclusive de inteligencia estratégica, etc. Todos estos datos están almacenados en un espacio “no tangible”, su inherencia en el espacio real y en la vida de las personas es total. Estadísticas de *comScore* “señalan que existen más de quince millones de usuarios en Internet

³ Norton, Peter, *Introducción a la computación*, 6a. ed., México, McGraw-Hill/Interamericana Editores, 2006, p. 539.

a nivel mundial con un rango de edad mayor a los quince años y que tienen acceso desde su hogar o centro de trabajo⁴.

El aumento del acceso a Internet en México y el desarrollo de nuevas tecnologías informáticas han propiciado la aparición de nuevas formas de delincuencia. Estas modalidades son peligrosas, afectan bienes jurídicos fundamentales de las personas, se desenvuelven en el ámbito digital, buscan causar perjuicio y representan una amenaza significativa.

La problemática que enfrenta la sociedad debido a las nuevas conductas antijurídicas perpetradas a través de dispositivos electrónicos es seria. Numerosas personas pasan gran parte de su tiempo diario navegando por la web, compartiendo constantemente información personal, como sus rostros, fotografías, actividades diarias, preferencias alimenticias y detalles adicionales. La gravedad de la situación se intensifica debido a que un número significativo de usuarios de Internet son menores de edad, y su principal medio de comunicación en línea es a través de las redes sociales.

Para comprender que está ocurriendo en Internet, las redes sociales y las comunicaciones mediante teléfonos móviles y los riesgos a los que estamos expuestos, es necesario encuadrar la definición de ciberespacio. El ciberespacio es un entorno virtual de alta utilidad para las comunicaciones, sin embargo, permite condiciones de riesgo ya que un atacante puede estar en cualquier parte del globo⁵.

El efecto de la globalización ha permitido la proliferación de las conductas antijurídicas cometidas por los medios informáticos y la Internet; presentes en el ciberespacio, no pueden existir sin la presencia de este mismo, ya que es el medio imprescindible para que se ejecuten y se lleven a cabo su comisión. El ciberespacio posee de un fácil acceso haciendo que los internautas quieran permanecer a ese ambiente virtual, lleno de novedades, interacciones, versatilidad y anonimato.

El ciberespacio es donde se “ubica” la aldea global, concepto proveniente del hecho de que Internet permite la existencia de una verdadera aldea global, ya que crea toda una comunidad en el ciberespacio que pareciera no tener

⁴ López Calvo, Pedro, *Derechos humanos, victimología, terrorismo y sus diversas modalidades delictivas, secuestros, delitos informáticos y armas de destrucción masiva*, México, editorial Flores, 2015, p. 415.

⁵ Jeannetti, Elena, *De la administración pública de seguridad de la información*, Revista Examen, México, Año XXIII, Número 228, marzo 2014, p. 56.

fronteras, o por lo menos no las fronteras tradicionales geográficamente delimitadas⁶.

Dado que el ciberespacio carece de fronteras, la criminalidad en línea también se despliega sin limitaciones, una característica sobresaliente al abordar los cibercrímenes. Esto los vuelve potencialmente peligrosos, ya que existen individuos que navegan por la web con la intención de causar daño a otros, obtener beneficios económicos o simplemente por el placer de infligir perjuicio.

Internet representa de este modo una forma de atacar valores jurídicos protegidos: la libertad e intimidad sexual de los menores; el derecho al honor, la intimidad personal y familiar y a la propia imagen; la dignidad humana; o los derechos de la propiedad intelectual. Valores que eran susceptibles de ser atacados también fuera de las redes digitales, pero que se presentan especialmente vulnerables ante el uso de las nuevas tecnologías⁷.

La criminalidad en línea afecta múltiples los bienes jurídicos tutelados que se pueden atentar por medio de las nuevas tecnologías informáticas y las redes sociales. Un ámbito que requiere una atención particular debido a la gravedad de la situación es la preservación del bien jurídico de la paz y seguridad de las personas. Este aspecto involucra la violación de la intimidad y la sexualidad de las personas, siendo perpetrado a través del delito de ciberacoso.

El ciberacoso es una conducta cometida a través de los medios informáticos, la Internet, las redes sociales y medios de mensajería instantánea como *WhatsApp*, *Facebook*, *Messenger*, entre otros. Este tipo de delito se manifiesta en el ciberespacio y no puede existir por sí solo. A diferencia de delitos tradicionales que implican contacto físico, el ciberacoso requiere la presencia de elementos específicos: ciberespacio, usuarios de Internet, un ciberdelincuente y una víctima.

III. Ciberacoso como violencia digital en México

La violencia digital o cibernética, especialmente el delito de ciberacoso es una conducta que no debería existir. Todas las personas que navegan por la web tienen el derecho de hacerlo de manera segura, sin que nadie afecte su esfera jurídica o les cause daño. Con este

⁶ Flores Salgado, Lucerito, *Derecho informático*, México, Editorial Patria, 2009, p. 113.

⁷ Marín Peidro, Lucia, *Los contenidos ilícitos y nocivos en Internet*, España, Fundación Retevisión, 2000, p. 38.

contexto en mente y con el fin de abordar la problemática actual, comenzaremos por definir el ciberacoso.

Por ciberacoso podemos entender a cualquier acto de violencia sistemático, psicológico, físico o sexual que realiza una persona o un grupo de personas, dirigido hacia otra u otras personas, que no se encuentran en posición para defenderse, utilizando la información electrónica y medios de comunicación tales como e-mail, mensajería instantánea, mensajes de texto, blogs, teléfonos móviles, *websites* (páginas web) difamatorios para acosar, puede constituir en muchos casos un crimen informático.⁸

El ciberacoso es una conducta típica, antijurídica y culpable de carácter preocupante, pues se manifiesta con agresiones, insultos, asecho, amenazas, intimidación, difamaciones, divulgación o creación de información falsa con fines de desprestigiar a la víctima, en la cual se vale de Internet y dispositivos electrónicos, provocando un daño que puede ser en algunos casos irreparables. Este tipo de violencia digital es un delito que afecta a la víctima de diversas maneras como mental, emocional y físicamente, causando depresión, estrés, miedo, impotencia, nerviosismo, ira, coraje, molestia, enojo, temor, inseguridades, ansiedad, vergüenza de sí mismo e inclusive en el peor de los casos puede llegar a ocasionar un suicidio.

Dado que la ejecución del ciberacoso se realiza mediante dispositivos informáticos, Internet y redes sociales, se clasifica como un delito informático o ciberdelito. En este contexto, es fundamental definir con precisión el concepto de ciberdelito.

Cruz de Pablo expresa que delito informático son aquellas: conductas típicas, antijurídicas, culpables y debidamente sancionadas por el ordenamiento jurídico penal para cuya ejecución se valen de ordenadores, computadoras o cualquier otro mecanismo electrónico o informático, bien como medio, bien como fin, o mediante el uso indebido de los mismos⁹.

Cuando nos referimos a delitos informáticos, no debemos limitarnos a considerar que se trata de un único tipo de ilícito. De hecho, este término abarca una amplia variedad de delitos que se llevan a cabo a través de medios informáticos e Internet, cada uno con

⁸ Pardo Albiach, Juan, *Ciberacoso: Cyberbullying, Grooming, Redes sociales y otros peligros*, en García González, Javier (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*, Tirant Lo Blanch, España, 2010, p. 54 y 55.

⁹ Cruz de Pablo, José Antonio, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, España, Grupo Difusión jurídica y temas de actualidad, 2006, p. 20.

modalidades específicas de ejecución. Estos delitos afectan a diversos bienes jurídicos protegidos. El ciberacoso, en este contexto, se clasifica como uno de estos delitos, ya que utiliza tecnologías informáticas como medio para cometer el ilícito.

Se clasifican dos tipos de ciberacoso: el ciberacoso directo y el ciberacoso por delegación. El ciberacoso directo es el envío de mensajes directos a la víctima; el ciberacoso por delegación implica utilizar a otras personas para ayudar a acosar cibernéticamente a la víctima, ya sea con o sin el consentimiento de estos cómplices, en otras palabras, hacer que otras personas realicen el trabajo sucio. Este último es el más peligroso¹⁰.

Las manifestaciones del ciberacoso incluyen el *Cyberbullying*, *Grooming* y *Sexting*, cada una con características distintas en la forma de ejecutarse y en la víctima a la que afectan. A pesar de sus diferencias, todas comparten el mismo propósito: acosar utilizando medios informáticos como instrumento.

El Cyberbullying (ciberacoso) es el acoso que realizan los menores de edad a otros menores utilizando las tecnologías. El objetivo es acosar psicológicamente, humillar, vejar y atormentar a través de las redes sociales a otros menores, y, según su intensidad y repercusión, puede ser un delito¹¹.

Una de las formas en que se manifiesta el ciberacoso es a través del Cyberbullying, que destaca por ser especialmente preocupante, ya que tanto la víctima como el agresor son menores de edad. Antiguamente, el Cyberbullying era conocido como acoso escolar, ya que se llevaba a cabo físicamente hacia la víctima, manifestándose directamente en escuelas o instituciones académicas. Sin embargo, con la introducción de medios informáticos, Internet y las redes sociales, este delito ha adquirido una nueva modalidad, transformándose en lo que ahora denominamos Cyberbullying.

Para los menores de edad, ser víctimas de Cyberbullying ocasiona un daño psicológico inmenso, afectando la autoestima y la seguridad en sus relaciones con otros compañeros de clase. Esto conduce al aislamiento y la falta de amistades. Además, repercute en el rendimiento académico, ya que los niños y jóvenes pueden evitar ir a la escuela, sentirse desanimados para participar en clase, e incluso, en los peores casos, puede incidir en la deserción escolar. El impacto del Cyberbullying es tan severo que las víctimas o sus padres

¹⁰ Kowalski, Robin *et al.*, *Cyber Bulling el acoso escolar en la era digital*, trad. De Francisco Campillo Ruiz, España, Editorial Desclee De Brouwer, 2010, p.83.

¹¹ Cervantes, Pere y Tauste Oliver, *Internet negro*, Ediciones Culturales Paidós, México, 2016, p. 75.

pueden llegar a no querer que el menor regrese a la escuela debido al temor de que las amenazas virtuales se materialicen en la realidad.

Por otro lado, los ciberacosadores o depredadores en línea son adultos que tratan de convencer a un menor de un encuentro físico con fines sexuales o de violencia, es por eso que buscan víctimas fáciles. Es decir se aprovechan de niños débiles o confiados, con problemas en su casa y que pasan largas horas en internet sin supervisión¹².

La conducta descrita, conocida como Grooming, implica que una persona adulta actúa con dolo aprovechándose de la inocencia de un menor de edad para *ciberacosarlo*. En esta situación, el agresor romantiza a la víctima, intentando obtener fotografías o videos con contenido sexual. Si logra su objetivo, puede almacenar o vender dicho contenido como pornografía infantil o manipular a la víctima para un encuentro físico. Es importante destacar que esta forma de ciberacoso es la más peligrosa, ya que afecta a la víctima no solo en su intimidad, sino también en su sexualidad.

En el caso de la Sextorsión, se trata de una forma de chantaje sexual en la que los cibercriminales poseen contenido privado de los usuarios, generalmente fotos o videos, y los amenazan con hacerlo público en Internet a menos que las víctimas accedan a cumplir con ciertos favores, que en ocasiones son de naturaleza sexual¹³.

El *Sexting* o Sextorsión al igual que el *Grooming* es una conducta más en las que se manifiesta el ciberacoso, la diferencia entre las dos es que en el *Grooming* las víctimas son menores de edad y en el *Sexting* son mayores de edad. Este tipo de delito perjudica a la víctima directamente difamándola y avergonzándola públicamente. Esta modalidad de ciberacoso es comúnmente ejecutada por la expareja de la víctima, afectando la intimidad de la víctima al ciberacosar o amenazar virtualmente con difundir ese contenido de carácter íntimo.

Rivas Mayett quien a su vez cita a Gabriel García Cárpoli, expresa que, se dividen a las víctimas susceptibles a un daño por medio de delitos informáticos en la siguiente clasificación: 1. Víctimas consientes: como aquéllas que en la comisión de un acto delictivo toman su conciencia de calidad de víctimas; 2. Víctimas inconscientes: aquéllas que no conocen de su situación de tales hasta

¹² Rivas Mayett, Diana, *Cibercriminalidad en México*, México, Servicio express de impresión, 2012, p. 85.

¹³ <https://www.ameci.org/index.php/acerca-de-ameci/chicos-ciberseguros/blog-ninos-ciberseguros/que-es-la-sextorsion>

un tiempo considerable del hecho delictivo o bien nunca llegan a conocerlo;

3. Víctimas penales: aquéllas que si son conscientes de su condición de víctima y reciben protección penal; y 4. Víctimas civiles: aquéllas que por razones de normatividad quedan fuera de la protección normativa¹⁴.

En el supuesto del delito de ciberacoso las cuatro víctimas se encuentran presentes, pues tenemos a la víctima consiente como la que sufre del ciberacoso; la víctima inconsciente como la que no conoce del hecho porque no tiene medios informáticos ni redes sociales, pero, si es víctima de ciberacoso porque en la red se encuentran amenazas e información de ella sin esta misma saberlo; la víctima penal como la persona afectada por la comisión del delito de ciberacoso y que presenta su querrela ante las autoridades correspondientes iniciando un proceso legal en contra del ciberacosador, y por último la víctima civil como la perjudicada del ciberacoso y quien busca presentar su denuncia ante las autoridades pero le es negada la protección judicial por falta de tipo penal correcto o falta de pruebas al hecho denunciado.

Cualquier individuo puede convertirse en víctima de ciberacoso, independientemente de su edad o si son usuarios activos de la red. Aunque es más común entre los jóvenes, las personas adultas no están exentas de sufrir este tipo de violencia digital. Por lo tanto, exploraremos el siguiente estudio estadístico para obtener una visión más amplia de la prevalencia actual de los casos de ciberacoso en México.

El Instituto Nacional de Estadística y Geografía (INEGI) realizó un estudio de análisis de ciberacoso en México, que comprende del 02 de agosto al 30 de septiembre de 2021, denominándose Módulo sobre Ciberacoso (MOCIBA) 2021. El objetivo de este trabajo de investigación de campo es dar a conocer información estadística sobre la situación del tema de ciberacoso en las personas de 12 años y más que usan internet en cualquier dispositivo, el cual, en modo de síntesis obtuvo la siguiente información:

La población usuaria de Internet que fue víctima de ciberacoso aumento de 21.0% en 2020 a 21.7% en 2021. En 2021, 22.8% de las mujeres y 20.6% de los hombres que usaron internet fueron víctimas de ciberacoso. La situación de ciberacoso más frecuente que experimentaron tanto mujeres como hombres fue el contacto mediante

¹⁴Rivas Mayett, Diana. *op. cit.*, p.33.

identidades falsas. La mayor prevalencia de ciberacoso se registró en Michoacán, seguido de Guerrero y Oaxaca¹⁵.

Con base en la información proporcionada, es evidente que el aumento de casos de ciberacoso está en aumento. Este incremento se ve influenciado por la creciente facilidad de acceso a Internet y dispositivos electrónicos. Dado que estos medios están al alcance de las manos y son las herramientas utilizadas para perpetrar el ciberacoso, su ejecución se vuelve sencilla y accesible. Esto provoca que cada vez se presenten más casos de este tipo de violencia digital.

Respecto de la identidad de la persona ciberacosadora, en el 59.4% de las situaciones de ciberacoso experimentadas no se identificó a las personas acosadoras, en 23% se logró detectar solo a personas conocidas. En 17.1% de las situaciones se identificó tanto a personas conocidas como desconocidas¹⁶.

El anonimato es una característica esencial que se presenta en los casos de ciberacoso, como se observa en la información proporcionada anteriormente. En la mayoría de los casos, la víctima no conoce a la persona que la ciberacosa, ya que no es necesario un encuentro cara a cara para que este tipo de delito se ejecute. En términos porcentuales, se encuentran personas que sí conocen a su agresor y pueden identificarlo, incluso presentando pruebas del delito. Por último, con el menor porcentaje en la estadística, están las víctimas que son ciberacosadas por personas que solo conocen virtualmente, sin tener un contacto en la vida real.

Viendo la magnitud del problema podemos señalar que es necesario ser cuidadosos con la información que subimos a Internet y redes sociales, no tener desconocidos como “amigos” en nuestras redes sociales, es importante para evitar ser víctima de ciberacoso, así como también bloquear a las personas que envíen mensajes indeseables, denunciar tanto en la red social como ante las autoridades de justicia penal, y actuar en temas de ciberseguridad.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, medidas de seguridad, pautas de gestión de riesgos, enfoques, acciones, capacitación, mejores prácticas, la garantía y tecnologías que pueden utilizarse para proteger el ambiente cibernético¹⁷.

¹⁵ Instituto Nacional de Estadística y Geografía INEGI, Modulo sobre ciberacoso 2021, México, Comunicado de Prensa Núm. 364/22, 13 de julio de 2022, p. 1.

¹⁶ *Ibidem*, p.15.

¹⁷ López Calvo, Pedro, *op. cit.*, p. 443.

Todas las personas internautas debemos de tener conocimientos en temas de ciberseguridad, dado a que queremos ser parte del ciberespacio necesitamos conocer cómo protegernos de amenazas para evitar que nos afecten, por ello, es importante evaluar qué información subir a las redes sociales antes de hacerlo, no aceptar solicitudes de amistad de personas desconocidas, no compartir contraseñas con nadie y cambiarlas frecuentemente, de esta manera estaremos más seguros al momento de navegar por la red, así como también tenemos que informarnos acerca del tema para saber cómo actuar en dicha situación.

El ciberacoso es una forma de violencia digital que debe detenerse. No es aceptable que estos delitos aumenten cada año. Es crucial concientizar a la sociedad sobre las graves consecuencias que esta conducta puede tener tanto para la víctima como para el ciberacosador. No debemos tomarlo a la ligera, ya que se pueden tomar medidas legales punibles.

IV. La tipificación del ciberacoso en México

La ley penal se enfrenta a una criminalidad en constante evolución, hace unas décadas atrás el legislador no se planteaba el supuesto de hecho que el delito de acoso se iba a cometer por los medios informáticos, ante estos tipos de delitos novedosos que cada vez se renuevan se necesita también que la ley penal se actualice para que estas conductas ilícitas encuadren correctamente al tipo penal legal.

La creación de tipos delictivos no puede ser una actividad que se someta al capricho temporal de una sociedad determinada. Consideramos por tanto necesario asistir a un somero estudio de la creación e interpretación de la ley penal para arribar a la conclusión de que la ley penal no debe ser –y menos en casos como este– tan relativa para fragmentarse en un punto geográfico a otro. Sin pretender obtener la ley absoluta, debemos aspirar a la creación de la ley más eficaz y amplia¹⁸.

A grandes rasgos, para crear tipos delictivos se necesitan de estudios que demuestren la incidencia delictiva de los hechos. Las leyes penales vigentes en un momento determinado conforme a la época se reforman para adecuarse a la sociedad actual, y con el apoyo de la política criminal, quien tiene la obligación de estudiar los hechos delictivos y encuadrar esas acciones al marco legal existente, para evitar la impunidad de las nuevas conductas ilícitas.

¹⁸ Nava Garcés, Alberto Enrique, *Análisis de los delitos informáticos*, México, Porrúa, 2005, p. 35.

Las normas penales también contemplan el uso de las *TIC's* (Tecnologías de la información y comunicación) como simples medios o instrumentos que sirven y se utilizan para la comisión de conductas delictivas, y, en este sentido, lo que se castiga es el hecho realizado (amenazar, falsificar, calumniar, etc.) con independencia del mecanismo que se haya utilizado para llevarlo a cabo¹⁹.

En un análisis por el Código Penal Federal podemos observar que aún no tenemos legislación actualizada para la figura del ciberacoso pues la última reforma a este artículo fue el 23 de enero de 2009, pero si se encuentra legislación actualizada para la conducta ilícita de *Sexting*, por su parte, también encontramos legislación aplicable para la conducta ilícita de *Grooming*.

El acoso se encuentra legislado por el Código Penal Federal en el Título décimo octavo denominado Delitos Contra la Paz y la Seguridad de las Personas en el capítulo I Amenazas y Cobranza Extrajudicial Ilegal contemplado en el artículo 282, el cual nos dice: Al que de cualquier modo amenace a otro con causarle un mal, en su persona, en sus bienes, en su honor, o en sus derechos, o en la persona, honor, o bienes o derechos de alguien con quien esté ligado a un vínculo y al que por medio de amenazas de cualquier género trate de impedir que otro ejecute lo que tiene derecho de hacer. La punibilidad mínima para este delito es de tres días de prisión y la máxima es un año de prisión o de ciento ochenta a trescientos sesenta días multa.

Analizando el artículo 282 del Código Penal Federal podemos notar la expresión “Al que por cualquier modo”, lo cual, interpretando la ley penal podemos ver que se incluyen los medios informáticos como el modo de ejecutar este delito, así que cualquier persona que utilice un medio informático para acosar a otra incurre en el delito de ciberacoso. Otra cosa que destaca del texto legal es la punibilidad, ya que observamos que la sanción mínima es de tres días de prisión, lo que hace suponer que la punibilidad no es acorde al daño que recibe la víctima de ciberacoso.

Para encuadrar mejor los supuestos de hecho y la punibilidad adecuada para el delito de ciberacoso a la legislación penal federal, se necesita de una reforma a este articulado, dado que hay que expresar textualmente las palabras “medio informático” y no dejarlo a la exclusividad de la interpretación de la ley penal; debido a que hay que subsanar esa laguna

¹⁹ Menéndez Mato, Juan Carlos y Gayo Santa Cecilia, Ma. Eugenia, Derecho e informática. Ética y legislación, España, Bosch Editor, 2014, p.332.

jurídica y darle certeza jurídica, pues si un hecho no se encaja con exactitud al tipo penal vigente no puede considerarse como delito aplicando la expresión *Nullum poena sine lege* “no hay pena sin ley”, o bien el principio de legalidad “Todo lo que no está prohibido está permitido” contemplado en el artículo 14 constitucional párrafo tercero.

Por otra parte, la conducta ilícita de *Sexting* se encuentra regulada por los artículos 199 *octies*, 199 *nonies* y 199 *decies* del Código Penal Federal, los que fueron adicionados el 01 de junio de 2021 para regular aquellas conductas que afecten en contra de la intimidad sexual usando los medios informáticos para ciberacosar a la víctima.

El artículo 199 *octies* correspondiente al Título séptimo Bis denominado Delitos a la indemnidad de privacidad de la información sexual en el Capítulo II Violación a la Intimidad Sexual, nos dice: Comete el delito a la violación sexual, aquella persona que divulgue, comparta, distribuya, o publique imágenes, videos o audios de contenido intimo sexual de una persona que tenga mayoría de edad, sin su consentimiento, su aprobación o autorización. Así como a quien videografe, audiografe o fotografíe, imprima o elabore, imágenes audios o videos con contenido intimo sexual de una persona, sin su consentimiento, su aprobación o autorización.

La intimidad se identifica así con la capacidad de control de las informaciones que sobre uno mismo pueden tener otras personas o más exactamente con la posibilidad de determinar “cómo, cuándo, y en qué medida se comunica la información a otros”²⁰.

La ley penal tiene como finalidad proteger bienes jurídicos de las personas, siendo el bien jurídico tutelado el objeto material o inmaterial de la protección que otorga la ley penal reconocido por el Estado en las legislaciones vigentes, en el delito de *Sexting* se agrede en contra de la intimidad sexual de las personas al hacer pública las imágenes o videos de la víctima.

En relación con la conducta ilícita de *Grooming* se encuentra regulada por los artículos 202 y 202 *bis* del Código Penal Federal que hace referencia a la pornografía infantil, encuadra con el texto de la ley cuando una persona mayor de edad ciberacosa a un menor de edad por medio de las redes sociales y ganándose su confianza le pide fotografías o videos y este las almacena o las utiliza para lucrar con ellas.

²⁰ Morales García, Óscar, *Delincuencia Informática. Problemas de responsabilidad*, España, Consejo General del Poder Judicial, 2002, p. 86.

Todo Estado debe de estar en posibilidad de enfrentar las amenazas que atente contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y defensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio²¹.

Como refiere Nava Garcés el Estado como ente protector de bienes jurídicos tutelados tiene la obligación de procurar la paz y la seguridad de las personas que habitan el ciberespacio, por lo que se tienen que implementar políticas públicas que incluyan el tema del ciberacoso dado que este delito presenta un reto para el Derecho en cuanto a legislación e implicaciones procesales, todo esto con el propósito de evitar la impunidad del ciberacoso.

V. Conclusión

Mucho antes de que existiera Internet, el acoso ya se manifestaba de manera física, es decir, cara a cara. Hoy en día con la ayuda de los medios informáticos, Internet y las redes sociales, el acoso evolucionó, tomó una forma distinta para llevar a cabo su comisión formándose el delito de ciberacoso del cual muchas personas han sido víctimas de este tipo de conductas antijurídicas propiciando un daño a su paz, seguridad e intimidad.

Es crucial destacar la necesidad de educar a todos los usuarios de Internet y redes sociales, incluyendo niños, niñas, adolescentes, jóvenes y adultos, para que naveguen en la Red cuidando y protegiendo su vida privada, intimidad sexual e información personal, con el objetivo de evitar ser víctimas de ciberacoso o sextorsión. Es de suma importancia promover valores y políticas públicas que aborden el ciberbullying y el grooming en los centros educativos, concientizando a los estudiantes sobre la gravedad de burlarse de sus compañeros y la importancia de tener precaución al interactuar en redes sociales. Por último, es esencial fomentar una cultura de denuncia ante las autoridades competentes, respaldada por la recopilación de pruebas, con el fin de prevenir la impunidad en casos de ciberacoso.

VI. Referencias

Bibliográficas

CERVANTES, Pere y TAUSTE Oliver, *Internet negro*, Ediciones Culturales Paidós, México, 2016

²¹ Nava Garcés, Alberto Enrique "Internet en América latina y su regulación", en Nava Garcés, Alberto Enrique (coord.), *El derecho en la era digital*, México, Porrúa, 2013, p. 165.

- CRUZ DE PABLO, José Antonio, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, España, Grupo Difusión jurídica y temas de actualidad, 2006
- FLORES SALGADO, Lucerito, *Derecho informático*, México, Editorial Patria, 2009
- GARCÍA GONZÁLEZ, Javier (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*, Tirant Lo Blanch, España, 2010
- KOWALSKI, Robin *et al.*, *Cyber Bulling el acoso escolar en la era digital*, trad. De Francisco Campillo Ruiz, España, Editorial Desclée De Brouwer, 2010
- LÓPEZ CALVO, Pedro, *Derechos humanos, victimología, terrorismo y sus diversas modalidades delictivas, secuestros, delitos informáticos y armas de destrucción masiva*, México, editorial Flores, 2015
- MARÍN PEIDRO, Lucia, *Los contenidos ilícitos y nocivos en Internet*, España, Fundación Retevisión, 2000
- MENÉNDEZ MATO, Juan Carlos y GAYO SANTA CECILIA, Ma. Eugenia, *Derecho e informática. Ética y legislación*, España, Bosch Editor, 2014
- MIRÓ LLINARES, Fernando, *Internet y delitos contra la propiedad intelectual*, España, Edición Fundación Autor, 2005
- MORALES GARCÍA, Óscar, *Delincuencia Informática. Problemas de responsabilidad*, España, Consejo General del Poder Judicial, 2002
- NAVA GARCÉS, Alberto Enrique, *Análisis de los delitos informáticos*, México, Porrúa, 2005
- NAVA GARCÉS, Alberto Enrique (coord.), *El derecho en la era digital*, México, Porrúa, 2013
- NORTON, Peter, *Introducción a la computación*, 6a. ed., México, McGraw-Hill/Interamericana Editores, 2006
- RIVAS MAYETT, Diana, *Cibercriminalidad en México*, México, Servicio express de impresión, 2012

Hemerográficas

- INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA INEGI, Modulo sobre ciberacoso 2021, México, Comunicado de Prensa Núm. 364/22, 13 de julio de 2022
- JEANNETTI, Elena, De la administración pública de seguridad de la información, Revista Examen, México, Año XXIII, Número 228, marzo 2014

LEYES CONSULTADAS

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS (Última reforma 12 de abril de 2019)

CÓDIGO PENAL FEDERAL (Última reforma 06 de enero de 2023)

Sitios web

ASOCIACIÓN MEXICANA DE LA INDUSTRIA DE TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIÓN Y ELECTRÓNICA (AMEC). (06 agosto 2021). "¿Qué es la sextorsión?" en Chicos Ciberseguros. Recuperado de <https://www.ameci.org/index.php/acerca-de-ameci/chicos-ciberseguros/blog-ninos-ciberseguros/que-es-la-sextorsion>