

LOS CIBERCRIMENES Y SU CONFORMACIONLic. María de los Santos Torres Hernández¹Lic. Adelaida Rodríguez Contreras²Dr. José Antonio Morales Notario³

Resumen: El objetivo del presente documento es identificar los distintos tipos de crímenes cibernéticos que prevalecen en la actualidad, así como la forma de orientar a la sociedad, para evitar involucrarse en los mismos y conocer las legislaciones que existen en nuestro País al respecto, para estar preparados ante una situación de esta naturaleza. Es incuestionable que los delitos cibernéticos surgieron a partir de los avances e innovaciones tecnológicas, sobretodo del Internet, del que se derivaron sin duda alguna páginas electrónicas o redes sociales; por lo que las personas con la finalidad de estar a la vanguardia o nivel de la tecnología, se han involucrado en la misma a tal grado que parecieran ser esclavos de ésta, y es claro que no pueden evitarlo. El Internet ha permitido contar con más recursos para mejorar su productividad, desarrollo y comunicación entre sus semejantes, tales como las páginas

electrónicas que brindan servicios al público general, con la finalidad de efficientizar los tramites gubernamentales o bien por simple diversión; sin embargo, existen páginas electrónicas que tienen algún tipo de contenido atrayente tanto para el hombre, como la mujer o niños, los cuales son operados por grupos criminales que disfrazan dichas redes o páginas electrónicas con el objetivo de inducir a la trata de personas, narcomenudeo, secuestros, extorsión y violación. A través del internet obtienen información personal de quienes ingresan a las mismas, utilizando mecanismos para envolverlos poco a poco, hasta lograr incluso en robarle su identidad y tarjetas de crédito o incluso realizar acciones consideradas delitos.

Palabras clave: redes sociales, libertad, delitos.

¹ Licenciada en Derecho y egresada de la Maestría en Derecho de la División Académica de Ciencias Sociales y Humanidades de la Universidad Juárez Autónoma de Tabasco.

² Licenciada en Derecho y egresada de la Maestría en Derecho de la División Académica de Ciencias Sociales y Humanidades de la Universidad Juárez Autónoma de Tabasco.

³ Doctor en Derecho. Profesor Investigador de Tiempo completo en la División Académica de Ciencias Sociales y Humanidades de la Universidad Juárez Autónoma de Tabasco.

Abstract: The objective of this document is to identify the different types of cybercrimes that currently prevail, as well as the way to guide society, to avoid getting involved in them, to know the laws that exist in our country in this regard, and to be prepared in a situation of this nature. It is unquestionable that cybercrimes arose from advances and technological innovations, especially the Internet, from which undoubtedly derived electronic pages or social networks; so that people, in order to be at the forefront or level of technology, have been involved in it to such a degree that they seem to be slaves of it, and it is clear that they cannot avoid participate on illegal actions. The Internet has allowed to have more resources to improve its productivity, development and communication among its peers, such as electronic pages that provide services to the general public, in order to streamline government procedures or for simple fun; However, there are electronic pages that have some type of attractive content for both men, women and children, which are operated by criminal groups that disguise these networks or electronic pages with the aim of inducing human trafficking, drug-dealing, kidnappings, extortion and rape. Through the internet they obtain personal information from those who enter them, using mechanisms to wrap them up little by little, even to steal their identity and credit cards or even take actions considered crimes.

KeyWords: social networks, liberty, crimes

Introducción

El internet se ha convertido en la actualidad un importante medio de comunicación que permite la interacción entre seres humanos; debido a ello, se ha experimentado un cambio social, que es visto como el resultado de la acción comunicativa entre las personas; sin embargo, esta conexión se da entre redes neuronales de los cerebros que ven las posibilidades políticas que se generan a través del internet. Los cerebros son estimulados por señales que se transmiten a través de las redes de comunicación (Castells, 2012).

Esta nueva forma de comunicación es parte de las tecnologías de conexión en red que, al convertirse en una plataforma para la comunicación, se convierte en un instrumento muy valioso, pues proporciona el espacio adecuado para que esta práctica, en el devenir diario, evolucione a tal grado que difícilmente se puedan seguir sus pasos.

Tanto las redes como el lenguaje común, definen nuevas relaciones temporales y espaciales que deben ser replanteadas puesto que rompen con la continuidad histórica de los medios de comunicación masivos. A medida que la

sociedad avanza debido a fenómenos como la globalización y el crecimiento exponencial, ésta se desplaza cada día al ciberespacio en busca de información y conectividad; sin embargo, este fenómeno no es aislado, ni privilegia a un grupo determinado, puesto que, al ser un medio abierto a la población, también incursionan en el mismo, quienes buscan obtener un rendimiento delictivo, aprovechándose de los nuevos medios y herramientas del internet (Sierra C., 2017).

Estos grupos delictivos han desarrollado mecanismos, métodos y técnicas virtuales, para vulnerar cualquier sistema de seguridad, generando actos delictivos en el ciberespacio, lo que se traduce como cibercrímenes.

Es importante puntualizar que el ser humano en su afán de descubrir cosas nuevas y por la desmedida confianza que tiene en este tipo de recursos, se ha expuesto a perder incluso su libertad, seguridad y vida; todo sin pensar en que puede existir como consecuencia, personas mal intencionadas que buscan hacer un daño o cometer un delito, a través de las redes, dando nacimiento de esta forma, a la delincuencia cibernética, de la que hasta la actualidad existe escasa regulación jurídica que la sancione y castigue, porque las redes sociales o páginas electrónicas, operan sin

control alguno y no existe supervisión de su contenido y alcances.

La cibercultura

La historia humana ha dependido de un proceso de civilización, el cual, durante muchos siglos se focalizó, basándose principalmente en el clima y la localización geográfica. Esto permitió el desarrollo de la vida humana, la que buscaba una mayor independencia de la naturaleza, pero no de los demás seres humanos, pues era necesaria la comunicación. El ser humano se adaptaba al frío, al calor, a la humedad, a las alturas, a la sequedad, a la costa pero, tan pronto hizo su aparición al sociedad, se modificó y adaptó lo antes construido y se adaptó a esta nueva forma de desarrollo. Al nacer la idea de un ciberespacio, que tenía como antecedente a los primeros e incipientes medios electrónicos de difusión de la información, surgió una nueva forma de ecología, no natural, que cubrió la totalidad del planeta y desarrolló de manera vertiginosa, la vida cultural y todas las formas de civilización. Esta nueva ecología que emergió con su peculiar metabolismo civilizatorio de gran independencia de la naturaleza es el mundo digital (Sierra C., 2017).

Si bien es cierto, la cultura incluye el conocimiento, las creencias, el arte, la moral, el derecho o cualquier otro hábito y capacidad adquirida por el hombre como integrante de una sociedad, la cibercultura es utilizada para propagar todo tipo de conocimiento a través de las redes sociales. Esto es así, porque la primera permite la interacción con los demás desde un espacio más personal, físico, diferenciado, en el que es visible todos aquellos desarreglos culturales; en cambio, el internet unifica los criterios y las diferencias; y ese espacio vital construye una nueva identidad en la que no es necesario relacionarse de manera normal y fluida con los demás, sino que el contacto es inexistente. Todo esto, matizado y registrado en el área del lenguaje escrito y en ocasiones, derivado de la proximidad o lejanía, se refleja de manera verbal (Faura, 2017).

Ana María Fernández (Quiñones, 2005), al definir a la cultura, hace referencia a todo lo relacionado con la estética, los sentimientos y las costumbres e indica que éstos tienen relevancia y determinan la forma en como la colectividad reacciona ante la vida. Clifford Geerts indica que la cultura es un esquema históricamente transmitido de significaciones representadas en símbolos y de concepciones heredadas y representadas en

forma simbólica, utilizada por los hombres, quienes comunican, perpetúan y desarrollan su conocimiento y actitudes hacia la vida. No es una entidad que pueda atribuirse de manera casual a los fenómenos sociales o a modos de conducta, instituciones o procesos sociales; sino que está integrada por una serie de mecanismos de control, planes, recetas, formulas, reglas e instrucciones que rigen la conducta del hombre, el cual depende de estos mecanismos para ordenar su conducta.

La cibercultura hace referencia al cambio de la cultura generado por la interacción del hombre con los sistemas de control y comunicación; es decir, entre los seres vivos y las máquinas. Pierre Levy (2007) señala que la cibercultura es “el conjunto de técnicas (materiales e intelectuales), de las prácticas, de las actitudes, de los modos de pensamiento y de los valores que se desarrollan conjuntamente con el crecimiento del ciberespacio”. Ante ello, la cibercultura está conformada por elementos de carácter simbólico y por las técnicas con sus artefactos, conexiones y dispositivos electrónicos que contribuyen a la creación del ciberespacio.

En ese sentido, la cibercultura no es sólo la cultura del ciberespacio, sino una nueva forma de conceptualizar, aprender y

entender lo que está sucediendo en el mundo, en el ciber mundo y en el hiper mundo.

El Rol Que Juega El Internet En El Mundo Actual

El papel del internet y de la comunicación inalámbrica en el actual movimiento social en red es fundamental (Castells, 2012). Ni el internet, ni ninguna tecnología puede ser origen de una casualidad social. La comunicación a través de las redes surge originalmente como una medida preventiva, pues se quería evitar que la información se perdiera, en caso de un ataque militar a los Estados Unidos, los cuales, preocupados por las comunicaciones militares y académicas de ese país, crearon un medio de comunicación descentralizado que permitiera el flujo constante de información sobre su territorio, ante el temor de una bomba nuclear soviética que afectara sus telecomunicaciones (Sain, 2015).

En 1969, al percatarse de las ventajas que tenía la interconexión, se incorporaron diversas instituciones educativas norteamericanas, comenzando su expansionismo y posteriormente la internacionalización de la red sin nodos centrales, al establecerse la comunicación

entre naciones: Estados Unidos a través de sus universidades, la Universidad College of London de Gran Bretaña y la Norwegian Seismic Array de Noruega en 1973. Sin embargo, no es sino hasta 1982 (Trigo, S.F.), que se logró definir al internet como el conjunto de redes interconectadas mediante un protocolo de control de transferencia y Protocolo de internet (TCP/IP).

En otras palabras, el internet no es más que es una red integrada por la interconexión de cables y señales de telecomunicaciones que permiten la comunicación entre miles de redes y computadoras, a través de una tecnología común para la transferencia de datos (Zamora, 2014).

Hoy en día, el internet se constituye como una tecnología decisiva en esta era de la información, ya que opera en todo el mundo a través de plataformas de comunicación inalámbricas, que proporciona la posibilidad de generar una comunicación multimodal e interactiva en cualquier momento y sin límites espaciales (Castells, 2014).

Sin embargo, es fundamental hacer hincapié en el papel decisivo de la comunicación en la formación y práctica de los movimientos sociales, toda vez que las personas se conectan entre sí y a través de

las redes sociales comparten sus alegrías, su indignación, sus frustraciones, sus estados de ánimo, sus emociones, sintiendo la unión y construyendo proyectos alternativos para ellas y la sociedad en su conjunto.

La información que se produce y maneja en las redes sociales, requiere de tecnología y medios que permitan hacer su uso de inmediato. Generalmente se hace de manera inconsciente y como un acto reflejo, sin analizar el fenómeno ni sus implicaciones. De los medios de información de 1969 a los actuales, existe una evolución dada de manera vertiginosa y casi inalcanzable que ha dado como resultado que los teléfonos actuales permitan el acceso al internet y a otras redes. Aunque esta depende de las telecomunicaciones, los satélites, los medios y las tecnologías, la información fluye, sin importar la existencia de fronteras territoriales. Y, si bien es cierto, inicialmente esta forma de comunicación estuvo reservada al alcance de un grupo social con poder adquisitivo suficiente para la obtención de estos aparatos, actualmente, no se puede excluir a nadie, salvo por la falta de conocimientos en informática (Morales C., 2004)

No se puede dejar de lado, que el internet se ve influenciado por factores económicos, pues a partir de éste, las redes

de telecomunicaciones, la informática y la información manejadas por los grandes bloques de la economía promueven diversos productos culturales que compiten o conviven con los locales; y de manera paulatina van colocando sus productos y sus precios; lo que permite una convivencia multicultural e interacción económica, política y social.

Al vivir dentro de un mundo de información, la percepción de los seres humanos se ha transformado. La realidad actual no es la de la colonia en la que radicamos, la ciudad donde vivimos o el país donde radicamos. Los numerosos mensajes que se reciben todos los días, provienen de diversas latitudes y en ocasiones no se logra identificar el origen del lugar de donde provienen tales informaciones, las cuales, en la mayoría de las ocasiones, se da por cierta, sin verificarse la fuente.

El derecho a la información sólo encuentra sus límites dentro del respeto a los demás, y en temas como el honor, la intimidad o la propia imagen. Es importante puntualizar que este derecho presupone el deber de todos los ciudadanos de informar objetivamente, sin embargo, la normatividad existente se ha rezagado de manera considerable en las prácticas cotidianas (Abba, 2005).

El Estado produce, acumula e informatiza datos de muy variadas clases, tipos e importancia, de manera continua y de acuerdo al funcionamiento de los órganos que la integran. Ante esto, toda información que produzca será útil para los ciudadanos y en consecuencia, debe serles accesible. Muchos países han reconocido en sus legislaciones que es necesario permitir que los ciudadanos accedan, de forma directa o a través de los órganos jurisdiccionales a toda información que pueda interesarles o perjudicarles, ya sea porque afecte su imagen, su intimidad o su vida privada. En este sentido, es claro que sólo se puede limitar el derecho a la información por excepcionales casos de seguridad.

Lo cierto es que, en la actualidad, las tecnologías de la información y la comunicación (TIC) ocupan los espacios de poder en un mundo global, además de que crean un canal privilegiado: “aldea global”, “sociedad global de la información”, “sociedad de la información”, “sociedad del conocimiento” entre otros, pretenden agrupar las relaciones o menos contradictorias entre un sistema técnico, un modelo cultural y un proyecto de organización de la comunicación.

En un principio, la información provenía de los países industrializados,

dónde destacaban los avances en el uso generalizado de la ciencia y la técnica, con altos niveles de investigación y desarrollo en tecnologías de punta, con la innovación y nuevos materiales de conectividad y energía, lo que permitió un salto cualitativo en las telecomunicaciones. Sin embargo, de acuerdo a Manuel Castells, la era de la información se desarrolló por tres procesos independientes: la revolución de la tecnología de la información, la crisis económica del capitalismo y el estatismo y el florecimiento de movimientos sociales y culturales como el antiautoritarismo, la defensa de los derechos humanos, el feminismo y el ecologismo; lo que creó una estructura social dominante, una nueva economía y una nueva cultura que tiene como base la virtualidad real (Hernández B., 2008).

En otras palabras, Mariano Palamidessi (2006) señaló que “la expansión de las tecnologías de la información y las comunicaciones han modificado de manera irreversible la vida de los países y las experiencias de las personas” y con estas tecnologías se busca agrupar, sistematizar y transferir todo tipo de información mediante la computación y las telecomunicaciones, además de que éstas van más allá del internet, del envío y recepción de mensajes. La web o red, busca

eficientizar y optimizar las comunicaciones (Pino O., 2011).

Sin embargo, la conectividad para el mundo globalizado depende de las redes interactivas de comunicación. Además, es a través de éstas que viven y actúan, obviamente en interacción, cara a cara y con la ocupación del espacio urbano. Las redes sociales digitales basadas en internet y en plataformas inalámbricas son herramientas decisivas para movilizar, organizar, deliberar, coordinar y decidir.

El papel de internet va más allá de ser un simple instrumento social pues crea las condiciones para que, de manera práctica, se puedan compartir movimientos sociales sin la necesidad de líderes, además de sobrevivir, deliberar, coordinar y expandirse. Este sistema es concebido como un medio de protección para el individuo en contra de la represión institucionalizada, ya que carece de espacios físicos liberados, a través de la comunicación entre la gente que la conforma y con la sociedad en general. Por ello, la sociedad en sí ve al internet como un medio por el cual puede crear una realidad paralela a la propia.

En la actualidad, el 97% de la información en el planeta está digitalizada, mientras que el 85% de esta es accesible a través de las redes de la información. A esto se suman el alrededor de 7 mil millones de

personas del planeta que cuentan con un celular y el 50% de la población adulta cuenta con un teléfono inteligente (Sánchez & Jiménez, 2015). Hay más de 3 mil 500 millones de usuarios de las redes sociales, las cuales se han transformado en un importante vínculo de comunicación no sólo en materia política -principalmente a la hora de emitir una opinión con respecto a la forma de gobernar- sino también en materia social.

Es importante destacar que existe una conexión fundamental más profunda, entre internet y los movimientos sociales en red debido a que comparten una cultura específica: la de la autonomía, que es considerada la matriz fundamental de las sociedades contemporáneas. Los movimientos sociales, si bien surgen del sufrimiento de la gente, son diferentes de los movimientos de protesta. Son fundamentalmente movimientos culturales, movimientos que conectan las demandas actuales con los proyectos del mañana. Éstos movimientos representan el proyecto fundamental de transformar a las personas en protagonistas de sus propias vidas afirmando su autonomía respecto a las instituciones de la sociedad.

La Importancia Del Internet

En el trasfondo de este proceso de cambio está la transformación cultural de las sociedades. Las características decisivas en este cambio dieron lugar al nacimiento de nuevos valores, tales como la individuación y la autonomía, los cuales tienen su origen en los movimientos sociales de los años sesenta y setenta y que dejaron una profunda huella en la sociedad que crecía con gran intensidad.

En ese sentido, la individuación es observada como la tendencia cultural que subraya los proyectos del individuo como principio esencial que orienta su comportamiento; por lo tanto, no puede ser confundida con el individualismo. El individuo puede estar dirigido a la acción colectiva e ideales compartidos, como la conservación del medio ambiente o la creación de una comunidad, y en el individualismo se hace referencia al bienestar del individuo, el objetivo último de su proyecto individuado (Castells, 2014).

La autonomía es un concepto que puede referirse tanto a actores individuales, como colectivos; sin embargo, es importante puntualizar que ésta se centra en la capacidad de un ser humano que decide convertirse en un sujeto definiendo su acción alrededor de proyectos contruidos al margen de las instituciones de la sociedad, de acuerdo con los valores e

intereses del propio actor social. El cambio de individuación a autonomía se realiza mediante la conexión en red, la cual permite a los individuos construir su autonomía con personas parecidas en las redes que elijan. Ante ello, el internet se convierte en una plataforma de comunicación organizativa que sirve para traducir la cultura de la libertad en la práctica de la autonomía (Castells, 2012).

Lo cierto es que las personas construyen redes para comunicarse y estar en contacto con otras, con las que quieren estar, o con quienes les gustaría conocer, partiendo del criterio que incluye a aquellas a las que ya conocen. Ante ello y al ser el internet una sociedad red autoconstruida, basada en la conectividad perpetua, ofrece a los usuarios un medio de comunicación idóneo que permite la interacción con cientos o miles de personas a través de su plataforma digital. Esto no significa que se trate solamente de una sociedad puramente virtual pues para quienes hacen uso de este sistema de interrelación, existe una estrecha relación entre las redes virtuales y redes de vida en general.

A más de 40 años del nacimiento del internet en –fijado en 1971 con el envío del primer correo electrónico-; a la fecha, existen 2,4 billones de usuarios. Yahoo se fundó en 1994 y un año después Microsoft

lanzó Internet Explorer. 1998 es un año importante para la historia de este importante medio de comunicación pues, además de que alcanza la ahora irrisoria cifra del millón de usuarios, nace Google, considerado con el tiempo como el gigante de las búsquedas; y en el 2001 que aparece Wikipedia, la mayor enciclopedia colectiva jamás creada. Las redes sociales también han evolucionado y entre 2003 y 2005 nacen programas específicos como Myspace, Facebook, YouTube, Flickr, Gmail, LinkedIn, Safari, Wordpress, Vimeo, entre otros. En el 2008 aparece Chrome de Google y dos años después, en el 2010, surge Instagram -aunque en su principio sólo era para Apple- y Pinterest, el cual consigue 10 millones de usuarios más rápido que otras redes (Infografías, 2013). La red ofrece la comunicación en el momento actual, sin importar la ubicación o localización de los participantes. Además, existen redes educativas, redes profesionales, redes de innovación, redes de entretenimiento, redes ciudadanas, redes socialización entre otras.

Especial atención merece Facebook, que nace en el 2004, que tuvo su mayor auge en el 2007 cuando se pudo traducir a muchos idiomas y tiene en la actualidad más de 2,000 millones de usuarios en todo el mundo (Sierra C., 2017). La mitad de ellos

navega a diario y el 50% actualiza su foto de perfil todos los días. A esta red se unen más de medio millón de usuarios diariamente y en los últimos años, su crecimiento en la población que oscila entre los 18 y los 24 años ha sido del 5%, entre los jóvenes de 25 y 34 años del 60%, y entre el grupo conformado de personas que están dentro de los 35 a los 54 de edad, del 190%. México es el primer país de América Latina en Facebook, con cerca de 30.0 millones de usuarios y la mitad son mujeres.

Facebook no ha permanecido ajeno a los negocios y tomando en consideración el amplio número de usuarios que hacen uso de la red diariamente, desarrolló un sistema de publicidad que lo ha convertido en una importante red en el campo del marketing, derivado de igual forma, del interés de las empresas que al observar su influencia en la sociedad y la posibilidad de establecer un negocio en este medio, influyeron en la creación de Facebook Ads, un sistema de publicidad que contó con las herramientas creadas por Google, que agregaron a su interfaz y que permite a las empresas la incorporación a las redes sociales (Bahillo, 2018).

Es importante destacar que ya antes de que Facebook fuera utilizado como red social y como importante fuente generadora de comercio, existían eBay y Amazon, que

surgieron en 1995 y que estaban destinadas específicamente al comercio electrónico. Desde el punto de vista demográfico Wikipedia, Amazon, eBay, YouTube, Facebook y Twitter tienen en común que la mayor parte de su audiencia son mujeres, destacándose en primer lugar Twitter con 62%, seguida de Facebook (57%), YouTube (55%) y Amazon (55%). Existe un mayor equilibrio entre eBay y Wikipedia, que tienen una proporción de mujeres y hombres es del 52% y el 48% (Marketingdirecto, 2011).

Facebook es la red que más tiempo invierte de media los usuarios. Los internautas pasan entre media de 32 minutos en este portal 37 segundos por página vista. Los usuarios de Twitter invierten una media de 7 minutos en el portal y 51 segundo por cada página vista. Wikipedia es la más rápida al momento de cargarse, con 1,236 segundos. YouTube (1,457 segundos), eBay (1,665 segundos), Twitter (1,729 segundos) y Amazon (1,783 segundos), convirtiendo a Facebook en la más lenta, pues en promedio tarda en cargar de 2,025 segundos (Marketingdirecto, 2011).

En el 2016, Facebook lanzó la nueva función Market, disponible para Estados Unidos, Reino Unido, Australia y Nueva Zelanda, debido a que más de 450 millones de personas compran y venden productos

cada mes y la que permitiría comprar y vender entre particulares (Peco, 2016).

En este punto es importante acotar que la cultura de la libertad a nivel social y la cultura de la individuación y la autonomía a nivel de los actores sociales, dieron lugar a las redes de internet y a los movimientos sociales en red al mismo tiempo, que en muchos de los casos ha transgredido los derechos fundamentales de las personas, porque la fácil accesibilidad y confianza desmedida en las redes de internet, los ha envuelto a tal grado, que han sido objeto de una serie de crímenes cibernéticos, por lo cual abordaremos dentro del contenido de este trabajo éste tipo de delitos.

Cibercrimenes Su Definicion

El delito es definido como toda acción u omisión que sancionan las leyes penales; los códigos los diferencian en acciones u omisiones dolosas o culposas. Sancionado por el Estado, el cual, a través de su legislación interna, prohíbe las conductas que considera lesivas para la sociedad y que dañan el orden jurídico establecido (Diputados, 2018).

En ese sentido, el cibercrimen es considerado cualquier crimen que se lleva a cabo en línea o que ocurre principalmente en línea, es decir, a través de las redes creadas por internet. Estas conductas van

desde el robo de identidad y otras violaciones de seguridad hasta actividades como la pornografía vengativa, el acoso cibernético, el hostigamiento, el abuso e, incluso, la explotación sexual infantil. Los terroristas cada vez participan más en Internet y trasladan los crímenes más aterradores al espacio cibernético (Symantec, s.f.).

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) estableció en 1983 que el ciberdelito es considerado cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos (Piña, s.f.). Antonio Enrique Pérez Luño (1996) lo define como aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectar el funcionamiento de los sistemas informáticos. Y, Miguel Ángel Davara (2015) lo define como la realización de toda acción que, reuniendo todos los elementos que integran al delito, se lleva a cabo utilizando un elemento informático. Lo cierto es que los delitos cibernéticos incluyen cualquier comportamiento criminal en el que los sistemas informáticos como computadoras o cualquier medio o dispositivo electrónico, es utilizado como material, objeto o símbolo.

Existe una diferencia notable entre lo que es el delito informático, relacionado con la delincuencia patrimonial y socioeconómica y el resto de los delitos cometidos a través de la informática y que se vinculan con conductas que afectan la intimidad, la libertad tanto física como sexual. El delito informático es únicamente una forma de realización de distintos tipos delictivos que tienen algunos elementos en común: a) Conducta fraudulenta (uso indebido o fraudulento de elementos informáticos a través de la introducción o manipulación de hechos falsos); b) Instrumento (presencia de los componentes físicos y/o lógicos del sistema informático); c) Finalidad (obtención de un beneficio ilícito, directo o indirecto, no necesariamente patrimonial); y, d) Resultado (perjuicio, no necesariamente patrimonial, de tercero o de la colectividad) (Corcoy, 2007).

Los ciberdelitos son cometidos por delincuentes que abusan de su anonimato para realizar conductas que son violatorias de las leyes, y van desde vender ilegalmente drogas, armas, artículos robados, documentos de identidad falsificados, material derivado del abuso sexual de menores, entre otras conductas que lesionan la dignidad de las personas. Las redes sociales presentan una gran oportunidad

para los cibercriminales, ya que ofrecen una falsa sensación de seguridad y los usuarios son más confiados a la hora de compartir información personal.

Hoy existen delitos como fraude, robo, chantaje y falsificación, pero las primeras conductas indebidas o lícitas que se realizaron usando una computadora datan de la década de los 70 y era de carácter económico, destacándose el espionaje informático, que abarcaba en esa época la extracción de discos rígidos, robo de diskettes o copia directa de la información de los dispositivos, -el espionaje era comercial o industrial y su objetivo eran los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de dirección de los clientes corporativos. La piratería de software consistía en la copia no autorizada de programas de computadora para su comercialización. El sabotaje a base de datos digitalizados y la extorsión eran los delitos que más preocupaban a las organizaciones, por la alta concentración de datos almacenados en formato digital. Los fraudes de tipo financieros consistían en la alteración de archivos de las bases de datos de las empresas y los balances de los bancos los cuales eran manipulados para alterar las

facturas de pagos de salarios (Parada, 2018).

Los casos típicos de delitos informáticos se realizaban mediante la instalación de dispositivos lectores en las puertas de entrada de los cajeros automáticos y teclados falsos con los que realizaban una copia de los datos de las tarjetas de débito que aparecían en la banda electromagnética. Esto obligó a las empresas y a los bancos a adoptar medidas preventivas como la adopción de chips en los plásticos y brindar cobertura legal de sus bases de datos, pues era indispensable otorgar seguridad a los usuarios de los servicios bancarios y empresariales en la realización de sus negocios y evitar el robo de información comercial.

En la década de los 90 y ante el desarrollo del comercio electrónico, la industria editorial, discográfica y cinematográfica, los derechos de autor se vulneraron a partir de la descarga e intercambio en línea de obras digitalizadas, música y películas. De igual forma se abrió la posibilidad de construir identidades ficticias alrededor de entornos virtuales en el internet. Sin embargo, algunas conductas causaron preocupación en el mundo virtual al existir un rebrote de pedofilia que inundó la red mediante la distribución de imágenes de pornografía infantil (Parada, 2018).

En la actualidad, los delitos informáticos se han clasificado de diversas maneras: existen conductas criminales de cuello blanco, como el hacking (acceso no autorizado a un equipo o sistema informático), cracking (vulneración del software comercial con fines de piratería informática), phishing (correos electrónicos y portales de internet falsos que en apariencia son enviados por instituciones o personas con las que se tienen contacto), evil twins (redes inalámbricas Wi-fi que aparentar tener conexiones a internet confiables), pharming (conducta criminal que desvía a un consumidor hacia una página electrónica apócrifa aún cuando se haya escrito correctamente la dirección electrónica de la página que se quiere contactar), spamming (envío masivo de información no solicitada por medio del correo electrónico), robo de identidad (no sólo contra personas físicas sino también jurídicas y en especial de derecho público), cyberterrorismo (posibilidad de ser atacado tanto los sistemas de información como las redes de datos o que estos sean utilizados por y para realizar actos terroristas), propagación de Malware a través de las redes de datos (Malicious Software, constituido por programas, documentos o mensajes que pueden causar daños a los equipos de los usuarios); el empleo de

tecnologías Pop-Up Ads y Adware (programas que se instalan con o sin el consentimiento de los usuarios informáticos, a través de ellos, se despliegan en intervalos de tiempo, anuncios y mensajes publicitarios que se sobreponen a la aplicación informática que se tenga en ese momento en uso), la instalación de Sniffers (usados para penetrar en el disco duro de los ordenadores conectados a la red, buscando cierto tipo de información), spyware (aplicaciones informáticas que recopilan información personal sin consentimiento del usuario) o programas espías de las computadoras personales para conocer los hábitos y actividades de familiares o empleados (que tienen como objetivo interceptar las comunicaciones establecidas entre los gobiernos, las organizaciones y las empresas de todos los países del mundo) (Piña, s.f.).

En ese mismo sentido, los delincuentes se segmentan por diferentes categorías, ya que los crímenes van más allá de dañar un simple computador. Se clasifican en: Programadores (generalmente hackers que se dedican a comprometer servidores y robar datos, crear Troyanos, amenazas y phishing, de igual modo, mantienen la seguridad de la infraestructura de los foros); vendedores de infraestructura

(proveedores de hospedaje que permiten contenidos ilegales que cuentan con una red muy vasta de equipos infectados y la ofrecen para hacer diferentes tipos de crímenes; venden computadoras infectadas, acceso a otros equipos, paquetes de infecciones, servicios de spam con enlaces de phishing o infecciones de troyanos, y servicios para ocultarse en la red); vendedores de datos (se dedican a traficar datos; venden sitios de comercio electrónico hackeados, direcciones de personas que les sirven para recibir mercancías robadas, tarjetas de crédito con datos personales, herramientas para averiguar si la tarjeta todavía está vigente, entre otros); defraudadores (pequeñas bandas hasta grandes organizaciones criminales compuestas por personas que se conocen en el mundo online pero que no se han visto físicamente; cada uno tiene una habilidad que encaja en la organización y entre sus servicios se encuentra la venta de tarjetas de crédito, servicios de llamada para finalizar transacciones y servicios de compra con números de tarjeta falsos y sólo participan profesionales) (Porfolio, 2012).

Existen riesgos relacionados con el uso de las redes sociales y esto se origina por el acceso que se tiene a todo tipo de información como lo es: el acceso a material

inadecuado, que va desde lo ilícito, lo violento, lo pornográfico, entre otros. El internet crea una adicción y en consecuencia distracciones para los usuarios; provoca problemas de socialización, robos de identidad, acoso, sexting, cyberbullying, cibergrooming. Estos tres últimos de reciente preocupación a nivel mundial, debido a que los delincuentes adquieren conocimientos técnicos que les permiten desarrollar herramientas que les permitan llevar a cabo sus objetivos y denigran y denostar, principalmente a las mujeres, niñas e incluso niños. Este tipo de amenazas crecen y evolucionan diariamente y a pesar de que los proveedores de las redes aplican filtros para evitar que estas conductas se realicen, la velocidad en la que crecen es vertiginosa y muchas veces no son posible de prevenir y evitar. La facilidad con que se puede contactar a cualquier persona en cualquier parte del mundo, ha contribuido a la globalización y al mismo tiempo, ha generado una cantidad importante de riesgos (Loredo G., 2013).

El Sexting, Un Peligro Y Riesgo Actual

En un principio, el internet se utilizaba en las computadoras fijas y esto focalizaba las conductas que se

consideraban dañinas para la sociedad; sin embargo, debido al desarrollo de las tecnologías, los celulares permiten la transmisión a nivel inmediato y desde cualquier parte del mundo. Esto ha provocado que conductas como el sexting y el grooming han prosperado.

El sexting es un fenómeno que surge a partir del uso de las tecnologías de la información y la comunicación combinado con cuestiones sexuales. Esta práctica está generalizada entre adolescentes, los cuales utilizan la cámara digital de su teléfono móvil para hacerse fotografías algo provocativas y en ocasiones, con contenido sexual explícito, que envía a un compañero o amigo con el que mantiene una relación sentimental. El problema radica cuando se concluye la relación y después de un tiempo, la fotografía es difundida entre amigos del chico, quienes la reenvían de forma indiscriminada o la suben a internet, donde la difusión se hace incontrolable. Es ahí donde empieza un verdadero calvario para la persona que se tomó la fotografía y la envió pues su derecho a la intimidad se ve seriamente dañado; además de que puede ser objeto de acoso psicológico, humillaciones, descalificaciones o ciberbullying (Vagace D., 2013).

Otra de las consecuencias del sexting es el sextorsión o el reclamo o

condicionante para el acoso sexual, lo que demerita a la víctima y tiende a reducir su dignidad a la mínima expresión. Es importante puntualizar que el envío masivo de material de sexting sin el consentimiento del autor de la fotografía o video sexualmente explícito, es considerado como una forma de ciberbullying pues generalmente desencadena una especie de hostigamiento virtual hacia el protagonista de éste.

Existen factores claves que influyen en su descripción y en el daño potencial que causan al protagonista, como: que la imagen puede ser de producción propia, ajena, con el consentimiento del protagonista, o robada. El contenido de la imagen es de tipo sexual, aunque en ocasiones es difícil definirla como atrevida, erótica, pornográfica, etc., y posiblemente se pueda identificar o no al protagonista. Factores como la edad dificultan la determinación de un rango porque existen problemas debido a que es un fenómeno que puede afectar a cualquier persona, de cualquier edad.

Existen además otros aspectos que agravan el problema, como el no pensar en el riesgo potencial que se corre derivado de la percepción de que no se distingue entre lo público y lo privado y de las consecuencias directas que surgen del mismo fenómeno; de igual forma, esta conducta afecta

principalmente a las mujeres y a las adolescentes, las cuales consideran que tienen un mayor conocimiento del internet que la gente de antes; a esto se anexa una sexualidad precoz de la infancia y la inmediatez de las comunicaciones que brindan el acceso a las nuevas tecnologías con mayor disponibilidad, facilidad, portabilidad y economía; y que alientan a que las personas realicen sus impulsos sin medir las secuelas que dejará su acción (Fajardo, Gordillo, & Regalado, 2013).

El Sexting conlleva una serie de riesgos y si no se medita sobre las consecuencias, coloca a las mujeres, niñas y adolescentes en una situación de vulnerabilidad pues con éste se busca degradar y que la víctima pierda su privacidad, además de que, aparejado a éste, surge el grooming y el acoso cibernético.

Las propias redes sociales brindan el espacio idóneo para la proliferación de estas redes al ampararse en la libertad de expresión y en el anonimato, sin importar que se están realizando actos que denigran y denostan a las personas y ante la falta de una legislación que se avoque a prevenir y sancionar a quienes atentan contra la dignidad de los demás a través de sus publicaciones.

Esta no es una situación sin importancia, el Instituto Nacional de

Estadística, Geografía (INEGI) explicó que en México existen aproximadamente 65.5 millones de usuarios de internet, y los Estados con más ciberacoso son Aguascalientes, Estado de México, Quintana Roo, Puebla e Hidalgo, con niveles que van de 28.6 a 32 por ciento de los usuarios; el 24.5 por ciento de los usuarios de internet de 12 años o más fueron víctimas de alguno de estas acciones, en mayor proporción los hombres. 24.5 por ciento de los usuarios de internet de 12 años o más enfrentaron experiencias de ciberacoso- El 52.1 por ciento eran varones, mientras que el 47.9 por ciento mujeres. En el rango de 12 a 19 años, las mujeres fueron las más afectadas (Posada, 2018).

La violencia en las redes sociales no tiene límites y hacia la mujer suele ser más ofensiva que hacia los varones. Y, lamentablemente no hay quien se salve. Ha habido incluso famosas que han sido víctimas del sexting y sus imágenes han llegado a todos los medios de comunicación, como el caso de Jennifer Lawrence, Demi Lovato, Vanessa Hudgens, Scarlett Johansson (Toren, 2017), Selena Gómez, Victoria Justice, Ariana Grande, Jennette McCurdy (Salud180, s.f.) y Charlize Theron por citar algunas.

El sexting es una forma de violencia que se ejerce a través del uso de internet y

que afecta la vida privada y social de las víctimas, las cuales sufren de insultos, amenazas y exclusiones de grupos de redes sociales (Inmujeres, 2016) y en la mayoría de los casos, este fenómeno trae aparejada una connotada discriminación de género con conductas como amenazas, intimidaciones, publicaciones falsas, vergonzosas e íntimas sobre la víctima, sin que ésta pueda identificar a su acosados que se esconde en el anonimato, lo que dificulta su identificación.

No se puede dejar de señalar que esta conducta trasgrede los derechos de las mujeres y principalmente los ordenamientos jurídicos más importantes como la Convención Americana sobre Derechos Humanos, la Convención sobre la eliminación de todas las formas de discriminación contra la mujer (CEDAW) y su protocolo facultativo, la Convención Americana sobre Derechos Humanos y la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (Belem Do Pará) entre otros.

Es importante contar con un control adecuado de las redes sociales que evite que los derechos, principalmente de las mujeres sean violentados, considerando que la violencia contra ellas es una ofensa a la dignidad humana que trasciende todos los sectores de la sociedad y constituye una

manifestación de las relaciones de poder históricamente desiguales entre hombres y mujeres (OEA, 1994).

Propuesta

Con la finalidad de combatir los cibercrimenes, se deben formular estrategias para protegerla de este daño social. Los expertos aseguran que para minimizar la ciberdelincuencia se requiere de ciberpolicías cada vez más capacitados para enfrentar los delitos que se cometen y adoptar medidas para evitarlos o prevenirlos, tales como: Usar las redes sociales con precaución; compartir tus vacaciones cuando hayas regresado o hacerlo de forma privada con familiares y amigos y no dar pistas acerca de las fechas de salida y regreso; desactivar las conexiones inalámbricas, Bluetooth, Wifi o GPS; investigar y generar evidencias de los delitos cibercrimenes y principalmente, tener actualizado los software, sistema operativo, antivirus y parches ; capacitar a los empleados y hacer campañas de concientización.

Así mismo, se deben implementar leyes que castiguen severamente éste tipo de delitos, porque se encuentra de por medio la libertad, seguridad, economía y particularmente la vida de las personas.

Conclusión

En nuestro país existen divergencias legales que originan a menudo atipicidad para las investigaciones de éste tipo de delitos. El Código Penal Federal (Diputados, 2018) contiene un capítulo entero dedicado a definir y sancionar el acceso ilícito a sistemas y equipos de informática (también llamado cracking) a partir de la adición que sufrió el artículo 211.

Los artículos 211 Bis, 211 Bis 1 al 211 Bis 7, definen una variedad de delitos informáticos. Se tipifica como delito la revelación de secretos, cuando indica que “a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa”.

Es importante que, en México se informe, promueva y difundan los alcances del modus operandi de los delincuentes cibernéticos a través de los medios de comunicación y redes sociales, para que la población en general tome las medidas necesarias para evitarlos.

La universalización del Internet ha conllevado al nacimiento de distintos fenómenos y conductas atípicas, que traen

como consecuencia la vulneración derechos fundamentales, de nuestra sociedad y principalmente de nuestros niños, niñas y adolescentes.

Es importante que se tomen medidas serias por los cibernautas, con la finalidad de prevenir los delitos a los que están expuestos al usar el ciberespacio y la internet o cualquier sistema informático o cibernético; todo lo anterior derivado de la obligación del Estado Mexicano de prevenir, investigar, sancionar y reparar las violaciones de los Derechos Humanos (Herrera P., 2013).

Bibliografía

Abba, B. (2005). El derecho de la sociedad de la información: importancia de internet en el mundo actual. *Revista Interamericana de Educación para Adultos Vol. 27, núm. 2*, 232-234.

Bahillo, L. (16 de mayo de 2018). *Historia de Internet: ¿cómo nació y cuál fue su evolución?* Obtenido de Marketing 4 Commerce: <https://marketing4ecommerce.net/historia-de-internet/>

Castells, M. (2012). *Redes de indignación y esperanza: los movimientos sociales en la era de Internet*. Madrid: Nueva Alianza.

Castells, M. (2014). El impacto de internet en la sociedad: una perspectiva global. En *Cambio. 19 ensayos fundamentales sobre cómo internet está cambiando nuestras vidas* (págs. 127-148). Bilbao: OpenMind-BBVA.

Corcoy, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos. *Eguzkilore*, número 21, 7-32.

Davara R., M. (2015). *Manual de Derecho Informático*. España: Aranzadi.

Diputados. (05 de 11 de 2018). *Código Penal Federal*. Obtenido de Cámara de Diputados del H. Congreso de la Unión. Secretaría General:
http://www.diputados.gob.mx/LeyesBiblio/pdf/9_051118.pdf

Fajardo, M., Gordillo, M., & Regalado, A. (2013). Sexting: nuevos usos de la tecnología y la sexualidad en adolescentes. *International Journal of Developmental*

and Educational Psychology. Familia y educación: aspectos positivos, 521-534.

Faura, R. (2017). *Cibercultura, ¿Realidad o invención?* Cataluña: Universitat de Barcelona.

Hernández B., M. (2008). Sociedad de la información: internet, poder y sociedad civil. *Revista Venezolana de Análisis de Coyuntura*, Vol. XIV, Núm. 2, 195-2165.

Herrera P., A. (2013). *Nuevo Sistema Constitucional de Derecho Penal. Principios jurídicos que lo integran*. México: Flores Editor.

Infografías. (17 de 05 de 2013). *La gran evolución de internet desde su creación en 1969*. Obtenido de MarketingDirecto.co,; <https://www.marketingdirecto.com/actualidad/infografias/la-gran-evolucion-de-internet-desde-su-creacion-en-1969>

Inmujeres. (15 de 07 de 2016).

Desigualdad en cifras. Obtenido de Gobierno de la República. Instituto Nacional de las Mujeres: http://cedoc.inmujeres.gob.mx/documentos_download/BoletinN7_2016.pdf

Levy, P. (2007). *La cultura en la era del ciberespacio*. México: Anthropos-Universidad Autónoma Metropolitana .

Loredo G., J. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. *Celernet*, 44.51.

Marketingdirecto. (15 de 06 de 2011). *Parecidos y diferencias entre Wikipedia, Amazon, eBay, YouTube, Facebook y Twitter*. Obtenido de Marketingdirecto.com: <https://www.marketingdirecto.com/digital-general/digital/parecidos-y-diferencias-entre-wikipedia-amazon-ebay-youtube-facebook-y-twitter>

Morales C., E. (2004). Internet y sociedad: relación y compromiso de beneficios colectivos e individuales. *Revista Digital Universitaria*. Vol. 5, Núm 8., 2-10.

OEA. (09 de 06 de 1994). *Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la mujer "Convención de Belem Do Pará"*. Obtenido de Organización de Estados Americanos. Departamento de Derecho Internacional:

<http://www.oas.org/juridico/spanish/tratados/a-61.html>

Palamidessi, M. (2006). *La escuela en la sociedad de redes. Una introducción a las tecnologías de la informática y la comunicación en la educación*. Buenos Aires: Fondo de Cultura Económica.

Parada, R. A. (2018). *Ciberdelitos y delitos informáticos: los nuevos tipos penales en la era de internet*. Buenos Aires: Erreius.

Peco, R. (03 de 10 de 2016). *Facebook lanza su propio Wallpop*. Obtenido de La Vanguardia: <https://www.lavanguardia.com/tecnologia/20161003/41756213574/facebook-mercado-ventas-compras-internet-comercio-electronico-wallpop-ebay.html>

Pérez L., A. (1996). *Ensayos de Informática Jurídica*. México: Fontamara.

Pino O., P. (2011). Las tecnologías de hoy en un mundo globalizado. *Gestión y desarrollo*, Vol. 8, No. 1, 209-216.

Piña, H. (s.f.). *Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano*.

Obtenido de Orden Jurídico:
<http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf>

Portafolio. (13 de 08 de 2012). *El alto costo de los crímenes cibernéticos*. Obtenido de Portafolio:
<https://www.portafolio.co/economia/finanzas/alto-costo-crimenes-ciberneticos-104604>

Posada, M. (05 de 02 de 2018). *Aumenta Cyberbullying en México, dicen expertos*. Obtenido de La Jornada:
<http://www.jornada.unam.mx/ultimas/2018/02/05/aumenta-ciberbullying-en-mexico-dicen-expertos-4939.html>

Quiñones, F. (2005). De la Cultura a la Cibercultura. *Hallazgos, núm. 4, diciembre*, 174-190.

Sain, G. (2015). Historia de Internet (1). *Revista de Pensamiento Penal*, 1-3.

Salud180. (s.f.). *Famosas que han sido víctimas del 'sexting'*. Obtenido de Bienestar180:
<https://www.salud180.com/salud-dia-dia/galeria/famosas-que-han-sido-victimas-del-sexting#imagen-1>

Sánchez, J., & Jiménez, H. (12 de 09 de 2015). *La influencia del internet, clave en la comunicación actual*. Obtenido de El Universal:

<https://www.eluniversal.com.mx/articulo/nacion/sociedad/2015/09/12/la-influencia-de-internet-clave-en-la-comunicacion-actual>

Sierra C., F. (2017). *Ciudadanía, tecnología y cultura*. Barcelona: Gedisa.

Symantec. (s.f.). *De qué manera distinguir el cibercrimen y protegerse*. Obtenido de Norton:

<https://mx.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html>

Toren, D. (20 de 08 de 2017). *Estas famosas han sido víctimas del sexting*. Obtenido de Nosotras.com:

<https://www.nosotras.com/sexo/famosas-victimas-del-sexting-559475>

Trigo, V. (S.F.). Historia y evolución del Internet. *Acta*, 1-11.

Vagace D., B. (2013). *Análisis de conductas sexting que afectan a la convivencia en las aulas de segundo ciclo de ESO*. Badajoz: Universidad Internacional de la Rioja.

Zamora, M. (2014). *Informática*. México:
Universidad Autónoma del Estado de
Hidalgo.