Las TIC,
ciberdelitos, ciberdelincuencia y su impacto jurídico-social

ICT cybercrime, cybercrimes and their legal-social impact

Sergio Gabriel Vázquez Sánchez[1]

Voces y Saberes. Año 4 núm. 11 julio-octubre 2024

Resumen

Las Tecnologías de la Información y Comunicación han tenido un desarrollo y crecimiento agigantado, actualmente son utilizadas no sólo como un medio productivo, sino como un elemento que facilita la comisión de delitos a través de las mismas, toda vez que, por su propia y especial naturaleza brindan anonimato y son difíciles de rastrear, además de que el sujeto activo no necesita encontrarse en el lugar para desplegar la conducta, por lo que, a lo largo del presente documento, se explorarán tópicos como ciberdelito, ciberdelincuencia y el impacto que ha tenido en nuestro país la comisión de conductas delictivas a través de las TIC. Lo anterior, enfocado a determinar con argumentos sólidos la razón por la cual deben ser consideradas como medios comisivos, materiales e inmateriales, de delitos.

Palabras clave: Internet, Tecnologías de la Información y Comunicación (TIC), delitos

Abstract

Information and Communication Technologies had enormous development and growth, and are currently used not only as a productive means, but as an element that facilitates the commission of crimes through them, since, for Their own special nature provides anonymity and is difficult to trace, in addition to the fact that the active subject does not need to be in the place to display the behavior, which is why, throughout this document, topics such as cybercrime, cybercrime and the impact that the commission of criminal conduct through ICT has had in our country. The above, focused on determining with solid arguments the reason why they should be considered as material and immaterial means of committing crimes.

Keywords: *Internet, Information and Communication Technologies (ICT), crimes.*

[1] Maestro en Derecho por la Facultad de Estudios Superiores Aragón, Universidad Nacional Autónoma de México, autor del artículo "Medidas y órdenes de protección para garantizar una vida libre de violencia" publicado en 2023, por la revista académica "Voces y Saberes" de la FES Aragón.

Introducción

Las Tecnologías de la Información y Comunicación (TIC), han sido parte importante de la vida del ser humano, evolucionando desde su nacimiento hasta la actualidad, siendo un pilar fundamental en el desarrollo científico, económico y social. Tal es la importancia actual del uso de las telecomunicaciones que, a partir de 1947, la Unión Internacional de Telecomunicaciones (UIT) se convirtió en el organismo especializado de las Naciones Unidas, abarcando todo el sector de las TIC, desde radiodifusión digital a internet y, de las tecnologías móviles.

El internet como una herramienta de acceso a la información, también ha favorecido al desarrollo de las nuevas TIC. La rapidez de la difusión, comodidad y la amplitud de alcance nacional e internacional que facilitan las nuevas tecnologías, las colocan como un elemento básico o de primera necesidad para la sociedad.

En México con el desarrollo y crecimiento de internet, se ha incrementado la población usuaria de las Tecnologías de la Información y Comunicación (TIC), las cuales facilitan el acceso a la red, por lo que es un hecho notorio que adultos, jóvenes e incluso niños tengan acceso al contenido de la web mediante las TIC.

Actualmente, el uso generalizado de las TIC en las actividades cotidianas de la sociedad mexicana, así como, la tendencia de la digitalización, conlleva y facilita a que más personas estén conectadas a internet, lo que a su vez, propicia una dependencia de los sistemas de información en ciertos sectores de la sociedad, aunado lo anterior la importancia de las Tecnologías de la Información y Comunicación como un factor de desarrollo político, social y económico, así como, de herramientas de trabajo y estudio, fomentan el uso recurrente de las mismas, por lo que la información que estas manejan y su uso diario las ha convertido en un elemento básico en la vida cotidiana.

Según el comunicado de prensa núm. 352/21 del Instituto Nacional de Estadística y Geografía (INEGI) correspondiente al 2020, en México actualmente existen 84.1 millones de usuarios de internet, lo que representa 72.0% de la población activa mayores de seis años[2]. Asimismo, dicho comunicado refiere que los tres principales medios para la conexión de usuarios a internet en 2020 fueron: celular inteligente (Smartphone) con 96.0%, computadora portátil con 33.7% y con televisor con acceso a internet 22.2 por ciento.

En México se encuentra consagrado el derecho a las TIC y a garantizar el acceso a internet, en nuestra Carta Magna, en su apartado dogmático, específicamente en el artículo 6 tercer párrafo, refiere que el "Estado garantizará el derecho de acceso a las Tecnologías de la Información y Comunicación, así como, a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet", por lo que podemos considerar como un derecho humano el acceso a las TIC.

Es preciso señalar, que dicho párrafo en el que se garantiza el derecho a las TIC, fue adicionado en el año 2013. Sin embargo, en la Constitución Política de los Estados Unidos Mexicanos, no se aprecia una definición o un concepto de lo que podríamos entender por Tecnologías de la Información y Comunicación.

No obstante, en la Ley de Gobierno Electrónico de la Ciudad de México publicada el 7 de octubre de 2015, se contempló una definición para las TIC, la cual continúa vigente en la Ley de la Ciudadanía Digital de la Ciudad de México, publicada el 9 de enero de 2020, misma que la define como un conjunto de dispositivos y sistemas

[2]Comunicado de prensa núm. 352/21, En México hay 84.1 millones de usuarios de internet y 88.2 millones de usuarios de teléfonos celulares: ENDUTIH 2020, https://inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

utilizados para almacenar, recuperar, procesar, transmitir y recibir paquetes de datos en formato digital. Por lo que, al realizar un estudio del concepto plasmado en la legislación local, podemos visualizar que cumple con los parámetros mencionados con anterioridad, es decir, refiere un tratamiento de información, mediante sistemas y dispositivos.

Ahora bien, con las definiciones de lo que son las TIC, consideraremos su alcance como medios comisivos de delito, es decir, el grado de participación que tienen en las conductas delictivas, la afectación que pueden generar al bien jurídico tutelado en la legislación penal. Al mismo tiempo, realizaremos un análisis del ciberdelito, ciberdelincuencia y evaluaremos el grado de importancia e impacto de las Tecnologías de la Información y Comunicación al momento de realizar la conducta típica.

El Ciberdelito

Actualmente podemos observar que el desarrollo tecnológico, la sed de información que tiene el ser humano, así como la presencia de las redes informáticas en cada rincón de nuestra vida cotidiana, han exigido de las Ciencias Sociales una actualización y consideración respecto a las relaciones humanas a través de las nuevas Tecnologías de la Información y Comunicación.
De forma similar, las TIC se han vuelto un elemento esencial en la vida cotidiana de la sociedad, al grado de ser omnipresentes y necesarias en el día a día de cada persona, no obstante, el crecimiento acelerado de esta sociedad de información se acompaña de nuevas e importantes amenazas.

La Ciencia Penal no se ha visto ajena a esta situación, ya que a través de los sistemas informáticos (*hardware*[3] y *software*[4]), se llevan a cabo diversas conductas constitutivas de delito. Al ser un fenómeno delictivo-social que va acentuándose y creciendo en cuanto a su propagación, es necesario observar las diversas definiciones que se han generado a partir de la pregunta ¿Qué es un ciberdelito o delito informático?

El principal aspecto negativo del desarrollo de las tecnologías informáticas, es que han abierto la puerta a conductas antisociales y delictivas, las cuales se han manifestado de maneras, que al día de hoy, era imposible imaginar. Lo anterior, al ser conductas antijurídicas que tienen impacto a nivel global, se considera necesario analizar las diversas concepciones que existen respecto a los ciberdelitos, mismos que no son cometidos por una computadora, es el ser humano quién haciendo uso de las nuevas TIC, ejecuta conductas antisociales con el objetivo de dañar o lesionar a la sociedad, mismas de las que hemos sido testigos con el paso del tiempo.

Tal situación no es un hecho aislado, toda vez que podemos encontrar diversos ejemplos de conductas ilícitas, realizadas mediante las Tecnologías de la Información y Comunicación. En Estados Unidos de América (EUA), se han documentado diversos casos de ataques económicos, a la información y a los programas computacionales, dentro de los más renombrados, podemos mencionar el golpe al *First National Bank* de 1988, el cual fue calificado como el esquema de malversación de fondos más grande en la historia de Chicago, considerando la cantidad de dinero que se sustrajo mediante transferencias electrónicas, aprovechando el acceso a los equipos informáticos, telefónicos y el conocimiento que poseían sobre el funcionamiento del sistema interno de transferencias[5].

Aunado a lo anterior, uno de muchos casos documentados en cuanto al robo de información, es el perpetrado en 1988 que sufrieron diversas agencias de gobierno, militares y empresas de Japón,

[3] Voz inglesa que se usa en informática para designar el conjunto de los componentes que integran la parte material de una computadora u ordenador, RAE, Diccionario panhispánico de dudas (PDP) [en línea], https://www.rae.es/dpd/hardware, 2 ed., consultado 06/05/24.
[4] Voz inglesa que se usa en informática, con el sentido de conjunto de programas, instrucciones y reglas para ejecutar ciertas tareas en una computadora u ordenador, RAE, Diccionario panhispánico de dudas (PDP) [en línea], https://www.rae.es/dpd/software, 2 ed., consultado 06/05/24.
[5] Menchaca, M., *Derecho Informático*, Bolivia, 2014, Creative Commons, p. 110

EUA y otros países, sin embargo, dichas afectaciones serán comentadas en el apartado referente al impacto social de los delitos cometidos mediante las TIC.

A nivel internacional, el marco de referencia con el que contamos es la definición brindada por la OCDE, en la que estableció que un *Computer crime* es cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos[6].

A su vez, la Unión Internacional de Telecomunicaciones, establece que el ciberdelito es "cualquier actividad delictiva en la que se utilizan como herramienta los computadores o redes, o estos son las víctimas de la misma, o bien el medio desde donde se efectúa dicha actividad delictiva, la cual puede realizarse a través de las redes electrónicas mundiales"[7]. Aunado a lo anterior, en el Convenio sobre la Ciberdelincuencia del Consejo de Europa, estableció una tipología al respecto, es decir, una clasificación sobre los tipos de ciberdelitos, considerándose los siguientes:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y los derechos afines.

A nivel nacional, en la Estrategia Nacional de Ciberseguridad (2017), se define como delitos cibernéticos o ciberdelitos a las "acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional"[8].

Sin embargo, a la fecha no se cuenta con una homogeneización respecto a la concepción técnico jurídica de lo que podríamos entender como ciberdelito, es decir, un concepto general que logre englobar la técnica informática, así como la problemática social y su regulación desde la dogmática jurídica, no ha sido definido.

Ahora bien, continuaremos el presente trabajo de investigación analizando las diversas definiciones y clasificaciones que tenemos respecto a los ciberdelitos, así como su grado de aceptación por parte de la doctrina.

Comenzaremos con la definición del Dr. Julio Téllez Valdés, quién en su obra de *Derecho informático* hace referencia a la complejidad de conceptualizar los delitos informáticos, toda vez que, para hablar de estos se requiere que sean acciones típicas y que, a su vez, se encuentren reguladas en la normatividad penal, lo anterior a fin de estar en posibilidad de catalogarlos como "delitos". Sin embargo, refiere que debido al grado de avance que ha tenido en la actualidad el uso desmesurado de las redes en la comisión de ilícitos, existe la urgente necesidad de catalogarlos dentro de la norma penal.

Por lo que los divide en concepto típico y atípico de la siguiente manera: concepto atípico, "delitos informáticos, son actitudes ilícitas que tienen a las computadoras como instrumento o fin", asimismo, en su concepción típica los concibe como "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin"[9].

A su vez, dentro de las principales características que tienen estos delitos informáticos según el Dr. Téllez Valdés, es que son, por lo regular conductas de cuello blanco, toda vez que, la persona que realiza su comisión requiere un cierto mínimo de conocimientos; llegan a generar grandes pérdidas económicas, ya que por lo general las personas que realizan este tipo de conductas buscan cifras que resulten atractivas; las denuncias al respecto llegan a ser mínimas comparadas

[6]OECD (1984) *Computer related criminality: analysis of legal policy in the OECD Area*, ICCP.
[7]UIT. *El ciberdelito: Guía para los países en Desarrollo*, División de Aplicaciones TIC y Ciberseguridad del UIT-D, abril 2009.
[8]Estrategia Nacional de Ciberseguridad, 2017, disponible en: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad
[9]Téllez, J., *Derecho Informático*, Mc Graw Hill, Instituto de Investigaciones Jurídicas, UNAM, México, 4 ed., 2009, p.188.

con la cantidad de casos registrados; son de carácter doloso y en la actualidad se da su proliferación principalmente entre menores de edad, debido a que son quienes desarrollan mayor facilidad en el manejo de los sistemas computacionales.

De la conceptualización anterior, así como de las características planteadas, consideramos que existen elementos susceptibles de resaltar, como el hecho de que son conductas (de carácter doloso), cuyo sujeto activo requiere un determinado conocimiento para su comisión y que tienen a las computadoras como un instrumento y/o fin de comisión.

Por otra parte, Rodríguez Davara refiere que el delito informático es "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 vulnerando los derechos del titular de un elemento informático, ya sea *hardware o software*"[10].

A su vez, Pérez Luño, sostiene que son "aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos"[11].

Asimismo, Pérez Llantada describe en un sentido amplio al delito informático como:

> cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el Delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin[12].

En relación con lo anterior, Sarzana proporciona una definición un poco más sencilla, pero no menos importante cuando menciona que son "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo"[13], lo anterior, si bien es cierto, proporciona un punto de vista general de lo que es un ciberdelito, brinda tres elementos a resaltar, los cuales utilizaremos para la formulación de nuestra propia conceptualización, conducta, criminal y computadora como material.

De lo anterior podemos mencionar que estas nuevas conductas criminales son definidas y denominadas por diversos autores de maneras distintas, algunos les llaman ciberdelitos, delitos cibernéticos, delitos informáticos, crímenes informáticos, lo que permite entrever que aún no existe un consenso respecto a la denominación, más aún, la conceptualización es diversa. Sin embargo, podemos advertir que, pese a no existir una homogenización respecto a la concepción de estos delitos, existen elementos que son concordantes.

En consecuencia y para la elaboración del presente trabajo de investigación vamos a usar el término ciberdelito, el cual vamos a entender como toda conducta desplegada dolosamente, cuya finalidad tiene la comisión de un acto ilícito, jurídicamente reprochable, realizada a través de las Tecnologías de la Información y Comunicación la cual puede ser con fines lucrativos o no lucrativos.

Ahora bien, debe hacerse la precisión para los fines de la presente investigación que, los delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella, como se ha mencionado anteriormente, es un hecho notorio que los medios tecnológicos actuales han contribuido enormemente a la sociedad, sin embargo, es necesario que se atiendan y regulen las consecuencias del uso indebido de los ordenadores y sistemas informáticos en general.

Dentro de las principales características de los ciberdelitos es que para que pueda darse la comisión de estos, el sujeto activo debe tener un cierto conocimiento y preparación al respecto, es decir, no

[10]Rodríguez, M., *Derecho Informático*, Aranzadi, Pamplona, 1993, p. 318
[11]Pérez, E., *Manual de Informática y Derecho*, Ariel, Barcelona, 1996, p.70
[12] Pérez, F., *Ciencias Penales, temas actuales*, edit. U.C.A., México, 2003, p. 583
[13]Sarzana, C., *Criminalita e Tecnología: il caso dei computer crimes*, Rassegna penitenziaria e criminológica, Roma, Italia, 1979, p. 59.


TOP
SECRET
CIBERDELITO

Voces y Saberes. Año 4 núm. 11 julio-octubre 2024

es una persona común y corriente, ya que, debe tener conocimientos especializados en materia de sistemas e informática, asimismo, estos delitos brindan al que los comete la facilidad de realizarlos desde cualquier lugar con conexión a internet, otorga un anonimato en su comisión, toda vez que, al cometerse mediante una conexión remota y un dispositivo con acceso a internet dificulta su rastreo, por lo que son un modo atractivo para aquellos criminales que buscan mantener el anonimato.

Cabe señalar que en los ciberdelitos no siempre el bien jurídico tutelado es el patrimonio, ya que, pese a que en la mayoría de las ocasiones los ciberdelincuentes buscan obtener un lucro, no necesariamente es la finalidad de los mismos, podemos observar que la criminalidad mediante el uso de las TIC, puede ir desde un fraude electrónico, hasta una usurpación de identidad o distribución de pornografía infantil, tráfico de personas, robo de datos personales, secuestro de información, lo cual vale la pena señalar, llega a ser en ocasiones más importante que el mismo daño patrimonial.

Un ejemplo de lo anterior podría ser el actual robo de datos que sufrió la Secretaría de la Defensa Nacional el pasado 6 de octubre de 2022, en el cual un grupo de ciberdelincuentes, sustrajeron información de carácter confidencial y de interés nacional. Si consideramos la gravedad del acto o el tipo de daño ocasionado, podemos deducir que, al ser una dependencia encargada de la seguridad nacional, la información con la que cuenta esa entidad es de interés y suma importancia para todos los ciudadanos del país.

Por lo que valdría la pena referir que, en cuanto a la protección del bien jurídico tutelado, debe considerarse la protección de los bienes jurídicos tradicionales y diversos, haciendo una reinterpretación teleológica de los tipos penales ya existentes, toda vez que, al realizarse una conducta delictiva pueden vulnerarse diversos bienes jurídicos tutelados en la norma penal, tales como:

*El patrimonio, es un hecho notorio y conocido que uno de los principales delitos cometidos mediante sistemas informáticos es el fraude electrónico y las manipulaciones de datos que pueden generarse, como ejemplo podemos observar la clonación de tarjetas y/o robo de cuentas bancarias a través de internet.

*La protección a la intimidad de datos, las agresiones informáticas afectan a la esfera íntima del gobernado en forma general, toda vez que actualmente la mayoría de las personas mantienen información de carácter privado y confidencial en sus equipos electrónicos, tales como, datos de tarjetas de crédito, ubicaciones de domicilios de familiares.

La propiedad considerada como patrimonio, se compone de los datos y documentos electrónicos (bienes intangibles) de carácter privado que tienen los equipos, hasta los daños a los mismos equipos, es decir, existen ocasiones en que los delincuentes cibernéticos, secuestran el disco duro (un bien tangible) y la única opción que queda al respecto es reemplazar el equipo.

Ciberdelincuencia

Una vez delimitado el concepto de ciberdelito, identificaremos lo que es la ciberdelincuencia y los factores que influyen en su comisión, así como los elementos que favorecen a que el fenómeno esté más vigente que nunca.

En el presente apartado revisaremos y analizaremos el fenómeno de la ciberdelincuencia, así como los factores que inciden en la comisión de este tipo de delitos, partiendo del hecho de que las redes de comunicación electrónica y los sistemas de información forman parte de la vida cotidiana de los seres humanos en el mundo, asimismo son parte fundamental en el éxito y desarrollo de la economía global.

En razón de lo anterior, vale la pena definir qué entendemos por delincuencia como fenómeno social, previo a poder estar en posibilidades de delimitar un marco conceptual para la ciberdelincuencia, según la RAE[14], es "Acción de delinquir", lo que nos lleva al significado básico de delito concibiéndolo como la conducta típica antijurídica y culpable, que significa una acción u omisión que es reprochada por la sociedad toda vez que, suele ser un hecho que pone en riesgo o vulnera derechos protegidos por su importancia.

Asimismo, la Constitución Política de los Estados Unidos Mexicanos nos otorga el concepto de lo que es la delincuencia organizada en el artículo 16, párrafo noveno, en el cual establece que debe entenderse como una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada. Por lo anterior podemos entender a la delincuencia como la comisión de delitos, es decir, la realización de conductas que la ley penal establece.

Ahora bien, al referirnos al prefijo que antecede a la delincuencia "Ciber" hace referencia al espacio cibernético o comúnmente denominado "la red", tal como lo mencionamos en el apartado anterior del presente trabajo, por lo que, podemos delimitar como ciberdelincuencia a las personas que despliegan una conducta criminal utilizando la red, es decir, realizan acciones que la ley penal establece como delitos a través de internet como un medio de comisión inmaterial, por lo que es factible referir que éstas personas cuentan con ciertas condiciones, conocimientos especializados o aptitudes que facilitan la comisión de los delitos a través de un medio tecnológico conectado a la red.

Uno de los factores fundamentales de la proliferación de este fenómeno delictivo es que la información tiene un valor económico importantísimo, considerando que el nacimiento y proliferación de este tipo de criminalidad viene de la mano con el desarrollo tecnológico. Las TIC son utilizadas para la comisión de diversos delitos, mismos que en su mayoría ya se cometían, pero se han ido perfeccionando con el uso y apoyo de los sistemas electrónicos que otorgan facilidades para la comisión y su anonimato.

Hace unos años en México el fenómeno de la criminalidad informática no había alcanzado una importancia mayor, pero hasta hace poco tiempo, con el desarrollo de las Tecnologías de la Información y Comunicación y el fenómeno de la pandemia por el COVID-19, fueron factores que favorecieron a la comisión de delitos mediante las TIC, asimismo, la poca denuncia de los delitos cibernéticos en nuestro país no refleja estadísticamente y de forma sustancial el incremento que han tenido estos delitos actualmente.

Diversos autores han referido que un elemento importante y que debe ser materia de análisis en cuanto a la comisión de ciber delitos es el sujeto activo, quien es aquel que despliega la conducta delictiva descrita en el tipo penal, lo anterior llama la atención toda vez que, para la comisión de este tipo de delitos se requiere un grado de especialización. Las personas que cometen Ciberdelitos, poseen ciertas características, cuentan con habilidades para el manejo de los sistemas informáticos y en ocasiones de acuerdo a su situación laboral se encuentran en posiciones estratégicas donde se maneja información de carácter sensible, por lo que se facilita la comisión de este tipo de delitos.

De conformidad con un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante computadora fueron ejecutados por empleados de la propia empresa afectada. Por otra parte, un estudio realizado en América del Norte y Europa, indicó que el 73% de las intrusiones informáticas cometidas eran atribuibles a fuentes interiores y sólo el 23% a fuentes externas[15].

[14] RAE, definición de delincuencia
[15] Acurio S., *Delitos Informáticos*, PUCE, p.15, 2019 recuperado de: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Voces y Saberes. Año 4 núm. 11 julio-octubre 2024

En su obra *Delitos Informáticos*, el Dr. Acurio del Pino refiere que, los criminales que realizan este tipo de delitos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, manifiesta que "el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por estabilidad emocional".

Tiedemann, en su obra *El concepto de derecho económico, de derecho penal económico y de delito económico*, refiere que:

> De manera creciente se emplea en la nueva literatura angloamericana el término "hecho penal profesional" (*Occupational Crime*). Con esta conexión al papel profesional y a la actividad económica, la particularidad del delito económico estriba ahora menos en la personalidad del autor y su pertenencia a la capa social elevada, y más en la especial manera de comisión (modus operandi), así como en el objeto de ese comportamiento"[16].

Por otra parte, se debe considerar a los ciberdelitos dentro de las formas de criminalidad de cuello blanco, porque desde un enfoque analítico criminológico, presentan las mismas peculiaridades que esta, con las salvedades que aporta la informática.

Se encuadra a los ciberdelitos con los delitos de cuello blanco derivado del hecho de que se requiere que el sujeto activo tenga un conocimiento especializado, este conocimiento favorece a que los sujetos puedan incidir criminalmente por medio de los equipos computacionales, razón de peso para considerar que los aspectos criminológicos como situación económica, factores sociales, carencia de oportunidades, por citar algunos, no son los factores que detonan el índice de criminalidad en este tipo de conductas.

A su vez, es preciso mencionar que este tipo de conductas delictivas han ido en incremento constante, afectando no solamente a un sector de la sociedad, es decir, el impacto que ha tenido el aumento generalizado en el uso de las TIC, ha propiciado que sean más comunes este tipo de delitos, incluso llegando al grado de cometerse en contra de dependencias estatales, como ejemplo basta mencionar el robo de información que sufrió la Secretaría de la Defensa Nacional en septiembre de 2022.

Consecuentemente, la ciberdelincuencia al ser un fenómeno criminal de alto impacto social, así como, una conducta que esta en constante incremento, debe estudiarse con la finalidad de que dichas acciones delictivas no queden impunes, más aún, considerando que en la norma penal por mandato constitucional, debe prevalecer el principio de la exacta aplicación de la Ley.

Impacto social de los delitos cometidos mediante las TIC

En México, así como en el resto del mundo los avances tecnológicos han sido de forma exponencial, beneficiando en muchas de las ocasiones a la sociedad, toda vez que, por lo general, representan un progreso en el estudio de diversas ciencias, por mencionar algún ejemplo, la medicina, la economía e incluso la investigación científica.

Sin embargo, el avance tecnológico ha traído consigo riesgos inherentes al uso de las Tecnologías de la Información y Comunicación, desde la seguridad de un país, hasta el riesgo que tiene un menor de edad con acceso a internet desde un *Smartphone*. Lo anterior podría parecer exagerado, pero basta con citar los ejemplos del robo de información ocurrido en 2016 mediante los denominados *Panama Papers* o la sustracción de información ocurrido en septiembre de 2022 a la SEDENA, mediante los cuales no sólo quedaron exhibidas las deficiencias en cuanto a seguridad cibernética de los Estados, también fueron filtrados documentos con carácter de Seguridad Nacional.

La transformación digital ha sido prioridad para diversos Estados, más aún con la pandemia generada por el virus SARS-COV2, la cual favoreció el uso de las

[16]Tiedeman, K., El Concepto de Derecho Económico, de Derecho Penal Económico y de Delito Económico, *Revista Chilena de Derecho*, Vol. 10, N 1, 1983, p 60

TIC como un medio alternativo para el desarrollo de las actividades económicas, laborales, sociales, políticas e incluso académicas.

El uso generalizado de las TIC en las actividades cotidianas de la sociedad mexicana, así como la tendencia de la digitalización, conlleva a un incremento de usuarios conectados a internet, incluso se ha generado una dependencia de los sistemas para el desarrollo de sus labores cotidianas, lo anterior favoreciendo a que el espacio cibernético sea susceptible de riesgos y una plataforma con extenso potencial para la criminalidad.

La rapidez de la difusión, el anonimato, la comodidad y la amplitud de alcance nacional y mundial que facilitan las nuevas tecnologías, hacen que los delincuentes aprovechen las mismas para llevar a cabo diversas actividades delictivas, dificultando su investigación por parte del Ministerio Público, así como, la tipificación de la conducta conforme a lo establecido en la norma penal, toda vez que, no es necesario que el delincuente se ubique físicamente en el lugar donde se comete el crimen o se localiza la víctima.

De acuerdo a como lo establece Miguel Estrada:

> la informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial, la idoneidad proviene básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos[17].

Es por las características que tienen las redes de internet, que el impacto social, así como el auge que han tenido la comisión de delitos a través de las redes, es prolífico, por lo que se puede considerar a las TIC como un medio idóneo en la comisión de cierto tipo de conductas ilícitas.

Téllez Valdés, al referirse a las características principales de los delitos cometidos mediante TIC, menciona situaciones concretas que tienen un impacto en la sociedad, tales como el hecho de que generan pérdidas económicas o que actualmente existe una incidencia al alza de los casos con una mínima cantidad de denuncias, ya que existe poca regulación en el Derecho al respecto de la comisión de las mismas, así como que existe la facilidad para que sean menores de edad los que las cometen.

Ahora bien, se ha considerado que las conductas delictivas realizadas mediante las TIC, conlleva a repercusiones que tienen un impacto social alto, sin embargo, pocas acciones se han implementado para prevenir o controlar este tipo de comisión de delitos, es decir, falta un grado de concientización social y de promoción de información que favorezca la prevención y por ende minimice el riesgo de su comisión.

Tal es el grado de impacto que han tenido las conductas delictivas en México, que de acuerdo con el reporte Tendencias de Seguridad en América Latina y el Caribe[18], el crimen cibernético ha generado un costo de entre 3000 y 5000 millones de dólares al año, si lo traducimos a un tipo de cambio de 18 pesos por dólar, nos da un impacto de 90 mil millones de pesos al año, tomando como referencia la cifra más alta. A su vez, en el resumen ejecutivo de la Estrategia Nacional de Ciberseguridad, el cual es un documento que plasma la visión del Estado mexicano respecto al incremento de riesgos, amenazas y ataques informáticos, así como, el incremento de conductas delictivas a través de las TIC, se estableció que estos riesgos pueden constituir un posible ataque a la dignidad humana, la integridad de las personas, a la credibilidad, reputación y patrimonio de las empresas, instituciones públicas y particulares, asimismo genera afectaciones a la seguridad pública o incluso a la seguridad nacional[19].

[17] Estrada, M., *Conductas Delictivas Informáticas*, Regulación Jurídica, 2019, UNAM, México, pp. 2
[18] Reporte Tendencias de seguridad en América Latina y el Caribe, OEA, disponible en el sitio de Internet: https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf consultado febrero 2023.
[19] "Estrategia Nacional de Ciberseguridad", 2017, México.

Voces y Saberes. Año 4 núm. 11 julio-octubre 2024

El uso de dispositivos electrónicos tales como, computadoras, teléfonos inteligentes, tabletas electrónicas, se ha incrementado en los últimos cinco años, ya que el costo de ellos ha disminuido, lo cual los hace un elemento común en la vida de las personas y con mayor facilidad de adquisición, además de que a través de ellos se pueden realizar distintas actividades entre ellas, operaciones bancarias, publicación de información desde personal, hasta contenido científico, incluso divulgación de datos de entidades del sector público.

A partir de 2015, el Instituto Nacional de Estadística y Geografía (INEGI) en conjunto con la Secretaría de Comunicaciones y Transportes (SCT) y del Instituto Federal de Telecomunicaciones (IFT), realiza la Encuesta Nacional Sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), misma que, desde ese año, capta las respuestas de diversos usuarios a nivel nacional, tomando en consideración la experiencia personal que cuentan en el uso de las TIC, considerando el aspecto socioeconómico del usuario y el tipo de población, permitiendo corroborar la disponibilidad y el uso de las TIC a nivel nacional.

Asimismo, el INEGI, con la finalidad de generar y conocer la información estadística que permitiera realizar una medición respecto al ciber acoso en México, implementó el Módulo sobre Ciberacoso (MOCIBA), el cual se agregó como módulo experimental a la ENDUITH, brindando sus primeros resultados en el 2017, a través de los que se conoció que al menos un 16.8% de la población de entre 12 a 59 años, han sufrido alguna vez "Acoso Cibernético". Lo anterior fue publicado en el "Comunicado de Prensa núm. 185/19", el 10 de abril de 2019, del mismo modo se obtuvo información respecto a que el uso de las TIC para la comunicación a través de redes sociales es especialmente popular entre los adolescentes y jóvenes, haciéndolos más vulnerables a sufrir situaciones relacionadas con el ciberacoso, toda vez que, dentro del rango de edad de entre 12 y 19 años, poco más del 20% de usuarios de internet señalaron haber vivido algún tipo de acoso cibernético.

Vale la pena mencionar que del análisis al Módulo sobre Ciberacoso realizado en 2017, se observan conductas que podrían considerarse como constitutivas de delito tales como: Suplantación de identidad, contacto mediante identidades falsas, llamadas ofensivas, insinuaciones o propuestas sexuales, envío y recepción de contenido sexual, publicación de información personal, críticas o burlas por apariencia o clase social y rastreo de cuentas o sitios web. De lo anterior se destaca que un factor clave para llevar a cabo dichas conductas de violencia virtual, es el anonimato con el que las personas pueden llegar a operar, toda vez que tienen conocimiento de la protección que brinda la red, lo anterior derivado del hecho de que el acoso cibernético no implica contacto físico entre víctima y agresor, ya que los medios electrónicos favorecen su comisión de manera encubierta, por lo que resulta complicado esclarecer la identidad de la persona que despliega la conducta.

En México, de acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019, se emitió el "Comunicado de Prensa núm. 103/20", del 17 de febrero de 2020, a través del cual el INEGI refirió que hay 80.6 millones de usuarios de internet, cifra que revela un aumento de 4.3 puntos porcentuales respecto a lo registrado en 2018 (65.8%), vale la pena destacar que el grupo de edad que

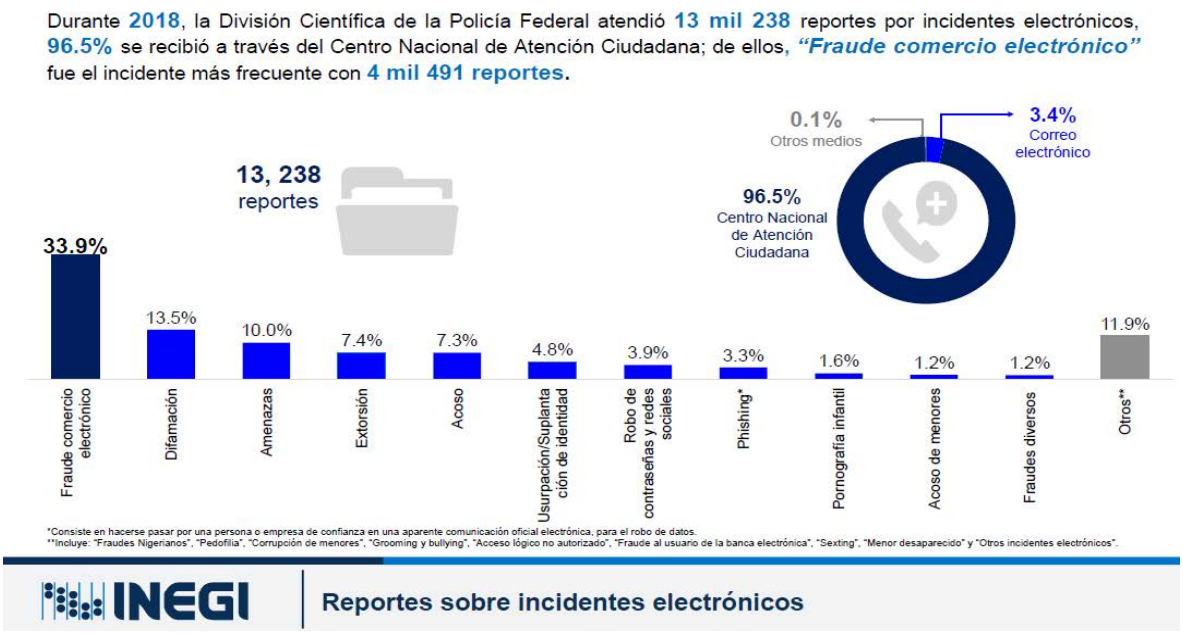
concentra la mayor proporción de usuarios de internet, corresponde al grupo de 18 a 24 años, teniendo estos una participación del 91.2%.

Siendo este un problema social, toda vez que existen diversos tipos penales ya establecidos en la norma que pueden cometerse mediante las Tecnologías de Información y Comunicación, no es solo un delito el que pudiera considerarse perpetrado mediante estos medios electrónicos, es decir, se pueden cometer delitos contra el patrimonio (fraude en diversas modalidades, robo, extorsión, usurpación de identidad, infracciones a derechos de autor), en contra de la libertad y el normal desarrollo psico-sexual (acoso, pornografía infantil, corrupción de menores, acoso de menores, pedofilia, sexting, violencia de género), en contra del honor (difamación, amenazas, discriminación, bullying) y en contra de la libertad de menores (menor desaparecido), por lo que la falta de regulación de las TIC como medios comisivos de delito, puede generar complicaciones en la impartición de justicia por parte del órgano jurisdiccional.

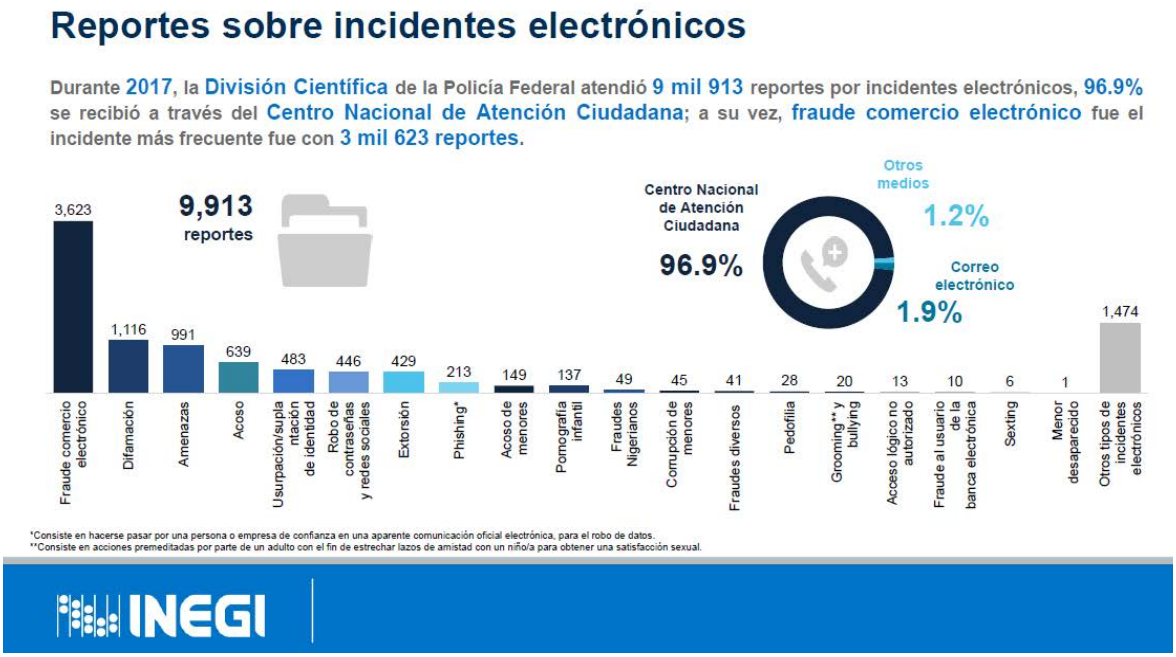
Al realizar el análisis de los tipos de delitos que podrían cometerse mediante las TIC, vale la pena plantear el siguiente cuestionamiento ¿Cuál es el método más eficaz de medir cuantitativamente y cualitativamente el impacto que pueden tener la comisión de delitos mediante las Tecnologías de la Información? De lo anterior, podemos determinar que la estadística sería la ciencia más apropiada para observar el grado de impacto, probabilidad de ocurrencia e incremento de las conductas ilícitas, por lo que, atendiendo a ese razonamiento, para la elaboración del presente trabajo de investigación, se consultaron fuentes gubernamentales con la finalidad de obtener cifras oficiales.

De acuerdo con la presentación de resultados generales del Censo Nacional de Seguridad Pública Federal correspondientes a los ejercicios 2018 y 2019, durante 2017, la división científica de la policía federal atendió 9 mil 913 reportes por incidentes electrónicos de los cuales fraude a comercio electrónico fue el incidente más frecuente con 3 mil 623 reportes, asimismo, durante 2018, la división científica de la policía federal atendió 13 mil 238 reportes por incidentes electrónicos, de los cuales fraude comercio electrónico fue el incidente más frecuente con 4 mil 491 reportes. De lo anterior, se desprende que hubo un incremento del 33.5% (3,325 reportes) respecto al ejercicio 2019 en comparación con el 2018.

Además, del análisis a los resultados generales del Censo Nacional de Seguridad Pública Federal de los ejercicios mencionados, se desprende que los reportes por incidentes electrónicos corresponden a la probable comisión de delitos en contra del patrimonio (fraude en diversas modalidades, robo, extorsión, usurpación de identidad, infracciones a derechos de autor), en contra de la libertad y el normal desarrollo psico-sexual (acoso, pornografía infantil, corrupción de menores, acoso de menores, pedofilia, sexting, violencia de género), en contra del honor (difamación, amenazas, discriminación, bullying) y en contra de la libertad de menores (menor desaparecido).



Fuente: Censo Nacional de Seguridad Pública Federal 2019, INEGI



Fuente: Censo Nacional de Seguridad Pública Federal 2019, INEGI

De los datos cuantitativos que se presentan en las tablas anteriores, podemos observar que la comisión de los delitos a través de las nuevas Tecnologías de la Información y Comunicación, ha tenido una tendencia a la alza importante y considerable.

Cabe resaltar que los datos presentados del INEGI, son derivados de encuestas realizadas a personas físicas, es decir, familias que han sufrido de alguna manera ataques a través de las Tecnologías de la Información y Comunicación, por lo que vale la pena considerar que las mismas no incluyen personas morales y/o sector gubernamental.

Según una nota publicada el 4 de junio de 2021, por el periódico El Financiero, las instituciones del sector financiero en México, durante el período comprendido entre 2019 y 2021, tuvieron más de 16 ataques cibernéticos, que se tradujeron en 785.4 millones de pesos, esto de conformidad con lo reportado por el Banco de México (BANXICO)[20], derivado en cierta manera del incremento en el uso de la banca por Internet.

Asimismo, de acuerdo con una nota periodística publicada el 20 de agosto de 2020, considerando datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), "en 2015, el número de quejas por fraudes cibernéticos se situó en las 790 mil 936, pero éstas se incrementaron sustancialmente: para 2019 fueron 5 millones 887 mil 729, hay un aumento de 664%"[21], lo anterior, denota un incremento importante en cuanto a la incidencia de este tipo de conductas criminales.

Aunado a lo anterior el Banco de México en el extracto del informe trimestral denominado "Información sobre los Ataques a Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI)", refirió que en el primer trimestre de 2018, tuvieron una incidencia de cuatro intentos de ataques cibernéticos a diferentes instituciones financieras, lo que pareciera ser un dato poco significativo, sin embargo, es preciso hacer mención que en el ataque perpetrado el 26 de abril del mismo año, se vieron afectadas tres instituciones bancarias, las cuales reportaron una pérdida de millones de pesos sin que pudiera encontrarse al responsable de la conducta delictiva.

A su vez, podemos observar que la comisión de delitos a través de las nuevas Tecnologías de la Información y Comunicación, no sólo han generado un impacto social a personas físicas y/o personas morales, tal es el caso de los ataques que a últimas fechas se han dado en dependencias gubernamentales, entre los cuales podemos mencionar el robo de información del que han sido víctima las dependencias de gobierno federal, entre las que destacan, el ataque a la Secretaría de la Defensa Nacional (SEDENA), del 30 de septiembre de 2022, Secretaría de Infraestructura, Comunicaciones y Transportes (SICT), 24 de octubre de 2022, Petróleos Mexicanos (PEMEX), noviembre de 2019, Secretaría de Economía (SE), 23 de febrero de 2020 y, el último caso a la Comisión Nacional del Agua (CONAGUA), 13 de abril de 2023.

De los ciber-ataques mencionados en el párrafo anterior, el que más ha causado daño y especulación es el perpetrado a la SEDENA, toda vez que, los ciberdelincuentes accesaron a documentación con carácter de Seguridad Nacional, es decir, tuvieron acceso a la base de datos, archivos y documentos clasificados por el ejército nacional como confidenciales, este ataque informático ha sido hasta el día de hoy, la más grave vulneración a la seguridad cibernética en México, lo anterior en virtud de que la información revelada comprende, desde el estado de salud del actual presidente de México, hasta operativos militares en contra del narcotráfico. Al respecto vale la pena resaltar que dicha invasión a los sistemas de seguridad informática del Estado, fue realizado por un grupo de hackers internacionales, lo que resalta una de las principales características de la comisión de ilícitos a través de medios electrónicos,

[20] Leyva, R., (2021, 4 de junio), "Reconoce Banxico 16 hackeos a bancos", [Articulo] *El Financiero*, http://elfinanciero.com.mx7economia/2021/06/04/reconoce-banxico-16-hackeos-a-bancos/
[21] Tapia, P., (2020, 20 de agosto) "Nos vaciaron la cuenta. Banorte, Santander y BBVA sucumben ante fraudes", [Artículo] *EME EQUIS*, http://m-x.com.mx/al-dia/nos-vaciaron-la-cuenta-banorte-santander-y-bbva-sucumben-ante-fraudes/

que es el hecho de que el sujeto activo en la comisión del delito puede realizarlo desde cualquier lugar con conexión a internet, situación que dificulta el rastreo y proporciona anonimato.

Asimismo, como último ataque a la seguridad cibernética nacional, podemos referir el realizado el 13 de abril de 2023, a la Comisión Nacional del Agua, en el cual fue secuestrada la información y documentación de la misma dependencia, solicitando un pago para su devolución, situación que imposibilitó realizar las actividades de dicho órgano desconcentrado y que puso en riesgo la información y documentación con la que cuenta a nivel nacional, hecho de gran importancia toda vez que, la comisión mencionada realiza actualmente obras en materia de infraestructura hidráulica con carácter de seguridad nacional, por lo que la comisión de éste tipo de ilícitos genera un daño quiza, de imposible reparación.

Lo anterior, denota que los ataques cibernéticos no sólo afectan al sector privado (personas físicas y morales), es un hecho notorio que los ciberataques van en aumento constante y causan un perjuicio a todos los sectores de la población, asimismo, el grado de sofisticación y daño generado es mayor, toda vez que, como se ha mencionado anteriormente, van desde daño patrimonial, hasta robo de información que puede comprometer la seguridad nacional.

A su vez, el desconocimiento sobre las amenazas, técnicas, metodologías, y herramientas que son empleadas por los ciberdelincuentes para la comisión de las conductas ilícitas, favorecen la proliferación de dichos ilícitos, aunado a la carencia de normatividad en México al respecto, como se hará referencia en el capítulo siguiente.

Conclusiones

Podemos observar que el impacto social que tiene la comisión de delitos a través de las Tecnologías de la Información y Comunicación, no es únicamente a las personas físicas, ya que, del análisis a la información contenida en el presente apartado, podemos observar que el daño puede darse tanto en el sector privado (personas físicas o morales), como en el sector público, poniendo en riesgo incluso información con carácter de seguridad nacional.

De acuerdo a lo anterior, si bien es cierto que la mayoría de este tipo de delitos tiene un móvil de lucro económico, se observa en los datos obtenidos del INEGI, que existen delitos cometidos mediante las TIC, que vulneran otro bien jurídico tutelado además del patrimonio.

Del análisis realizado, podemos determinar que la comisión de éste tipo de ilícitos no obedece edad, sexo, religión o grupo social, lo que favorece que cualquier persona de cualquier estrato social sea susceptible de ser víctima de algún ilícito a través de las TIC, aunado a lo anterior, podemos concluir que los delitos cometidos en su gran mayoría ya se encuentran descritos en la ley penal, por lo que se considera que valdría la pena tomar a las Tecnologías de la Información y Comunicación, como medios comisivos, es decir, mecanismos materiales e inmateriales a través de los cuales se perpetran estas conductas criminales.

La comisión de delitos o conductas posiblemente constitutivas de delitos mediante TIC, podrían encontrarse en la parte general del Código Penal, como una circunstancia agravante o como algún medio comisivo a través del cual se despliegue la conducta típica, a fin de agravar la penalidad impuesta al sujeto activo.

Lo anterior, con la finalidad de intimidar al posible delincuente, toda vez que, como se ha observado a lo largo del presente documento, aquel sujeto activo que es capaz de desplegar una conducta delictiva a través de las Tecnologías de la Información y Comunicación, es una persona con un grado de instrucción específico, es decir, conoce los alcances de la acción que despliega y en la gran mayoría de los casos desea el resultado material, por esto, es que se considera que el uso de las TIC como medios comisivos de delito debe ser previsto en la legislación penal, endureciendo la penalidad buscando inhibir e intimidar al criminal.

Referencias

Acurio,S., (2019), *Delitos Informáticos*. Recuperado de: http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599 pp. 12-15

Consejo de Europa - CdE. (2001). Convenio sobre la Ciberdelincuencia. Serie de Tratados Europeos No. 185. Budapest, Hungría: Publicación de la Secretaría del CdE https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Censo Nacional de Seguridad Pública Federal 2019 y 2018

Constitución Política de los Estados Unidos Mexicanos. Recuperado de: https://diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Diccionario Panhispánico de dudas (PDP). Recuperado de: https://www.rae.es/dpd/software

Estrada, M., (2019), *Conductas delictivas informáticas, regulación jurídica,* UNAM. México. p.2

Estrategia Nacional de Ciberseguridad, 2017. Recuperado de: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad

Instituto Nacional de Estadística y Geografía (INEGI) Comunicado de prensa núm. 352/21, *En México hay 84.1 millones de usuarios de internet y 88.2 millones de usuarios de teléfonos celulares: ENDUTIH 2020*. Recuperado de: https://inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

Comunicado de prensa núm. 103/20, del 17 de febrero de 2020. Encuesta Nacional sobre Disponibilidad y *Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2019*. Recuperado de: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf

Ley de Gobierno Electrónico de la CDMX. Recuperado de: https://congresocdmx.gob.mx/rchivos/legislativas/LEYDEGOBIERNOELECTRONICO-CDMX.pdf

Leyva, J., (2021, 4 de junio), "*Reconoce Banxico 16 hackeos a bancos*", [Artículo] El Financiero. Recuperado de: http://elfinanciero.com.mx/economia/2021/06/04/reconoce-banxico-16-hackeos-a-bancos/

Menchaca, M., *Derecho Informático*, Santa Cruz Bolivia, 2014, DL.8-1-740-14, P. 110

Organización de Cooperación y Desarrollo Económico (OECD) (1984) *Computer related criminality: analysis of legal policy in the OECD Area, ICCP*

Organización de los Estados Americanos, *Reporte Tendencias de seguridad en América Latina y el Caribe*. https://www.sites.oas.org/cyber/Documents/2014%20-%20Tendencias%20de%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe.pdf consultado febrero 2023.

Pérez, A., (1996) *Manual de Informática y Derecho. Barcelona*, p. 70

Pérez, F (2003). *Ciencias Penales, temas actuales*. UCA México. p. 583

Rodríguez, A., (1993) *Derecho Informático*, Pamplona, p. 318

Sarzana, C., (1979), *Criminalita e Tecnología: il caso dei computer crimes,* Rassegna, penitenziaria e criminológica. p.59

Tapia, P., (2020, 20 de agosto), *Nos vaciaron la cuenta. Banorte, Santander y BBVA sucumben ante fraudes*, [Artículo], EME EQUIS, http://m-x.com.mx/al-dia/nos-vaciaron-la-cuenta-banorte-santander-y-bbva-sucumben-ante-fraudes/

Téllez, J., (2009) *Derecho Informático*, Edit. Mc Graw Hill, 4 ed., p. 188

Tiedeman Klaus, (1983), El Concepto de Derecho Económico, de Derecho Penal Económico y de Delito Económico, *Revista Chilena de Derecho*.

Unión Internacional de Telecomunicaciones (UIT) El ciberdelito: Guía para los países en Desarrollo, División de Aplicaciones TIC y Ciberseguridad del UIT abril 2009.