UNIVERSIDAD AUTÓNOMA DE SINALOA

FACULTAD DE DERECHO, CULIACÁN

UNIDAD DE ESTUDIOS DE POSGRADO DE LA

FACULTAD DE DERECHO CULIACÁN

# "LA TIPIFICACIÓN DEL DELITO DE ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA EN MÉXICO"

TESIS

QUE COMO REQUISITO PARA OBTENER EL GRADO DE MAESTRA EN CIENCIAS DEL DERECHO

PRESENTA:

LIC. KARLA KARINA SÁNCHEZ VILLA

DR. FERNANDO CASTILLO LORA

DIRECTOR

Culiacán, Rosales, Sinaloa, Mayo de 2019

Dedico esta tesis:

A mi amado esposo por alentarme a estudiar una maestría, por ser mi pilar de apoyo, y por demostrarme que con trabajo y esfuerzo se logran excelentes cosas.

A mi mamá y a mis papás por formarme para ser una profesionista del derecho, muchos de mis logros se los debo a ustedes, entre los cuales destaca éste.

A mi hermana mayor por ser un ejemplo a seguir.

Y a mis hermanos menores con el objeto de mostrarles que el estudio les abre las puertas al mundo.

AGRADECIMIENTOS

Agradezco a la Unidad de Estudios de Posgrado de la Facultad de Derecho Culiacán, perteneciente a la Universidad Autónoma de Sinaloa, por darme la oportunidad de formar parte del plan de estudios de Maestría en Ciencias del Derecho, cultivando en mí la pasión por la investigación jurídica.

Al Consejo Nacional de Ciencia y Tecnología por el apoyo económico que me brindó en la duración de la presente investigación.

A mi director de tesis el Dr. Fernando Castillo Lora por las horas de atención brindadas, por compartir parte de su conocimiento científico-jurídico en la elaboración de este trabajo de investigación, por creer en mi capacidad académica, así como también por haberme tenido la paciencia para guiarme durante y hasta cumplir el término de este proyecto de tesis.

Quiero dar las gracias enormemente a mis lectores de tesis el Dr. Gonzalo Armienta Hernández y con mucho cariño a la Dra. María Teresa Guzmán Casillas, por el apoyo que me han brindado, por su disposición y por la colaboración presentada para la realización de este trabajo de investigación.

Muchas gracias.

ÍNDICE

# INTRODUCCIÓN

La tesis presentada con el tema: La tipificación del delito de Acceso ilícito a sistemas y equipos de informática en México, para optar por el grado de Maestra en Ciencias del Derecho, obedece la inquietud de que, en las últimas décadas las tecnologías informáticas se han propagado en una gran parte del mundo, proporcionándonos múltiples beneficios, por ejemplo: mantener resguardada información de diversa índole. Paralelamente a su incremento han surgido nuevas formas de criminalidad, las cuales, deben de tener una correcta tipificación; ante la ley penal de nuestro país estas se denominan como: delito de Acceso ilícito a sistemas y equipos de informática, el cual tiene como objeto proteger el bien jurídico de la información contenida en estos mismos.

La investigación de la mencionada problemática se realizó con la finalidad de analizar el marco jurídico vigente respecto al delito de Acceso licio a sistemas y equipos de informática en México, valorando si su tipificación es clara, si es la correcta, si es homologada en el territorio nacional, y si se encuentra análoga con la legislación de países como Alemania, Francia y España en relación a este delito.

Para explicar dicha serie de acontecimientos la tesis se estructura en tres capítulos. El primer capítulo denominado Internet e informática en el delito de Acceso ilícito a sistemas y equipos de informática, se atendió el concepto de la Internet e informática, los antecedentes que le dieron origen y la relación existente de estas tecnologías con el ciberdelito.

En el segundo capítulo nombrado: Conductas delictivas que afectan el secreto informático y su tipificación, se le dieron tratamiento a los temas del concepto de delito y a su vez el concepto de delito informático; posteriormente se analizó la legislación vigente sobre la tipificación de este delito tanto del Código Penal Federal, como en los diferentes Códigos Penales Estatales de México, con el propósito de determinar el marco jurídico de su regulación; también se precisaron las razones que dieron lugar a su tipificación; y la evolución y desarrollo de las figuras típicas de la informática en el Código Penal Federal.

Aunado a lo anterior también en el segundo capítulo se especificaron las diversas conductas con las que se comete este delito y su forma de ejecutarse, encontramos que son diversas las maneras con las que se afecta el bien jurídico de la información contenida en los medios electrónicos; y por ultimo de este capítulo se desarrolló el tema de las conductas no tipificadas que afectan bienes jurídicos fundamentales, las cuales son de urgencia que se contemplen en el Código Penal Federal.

Por otra parte, el capítulo tercero se centró en el ámbito internacional, denominándose: Los delitos informáticos en el Derecho Comparado, de esta forma, se analizó sistemáticamente y por orden cronológico cómo Alemania, Francia y España regulan estas conductas típicas, con el objeto de contrastar la figura del delito de Acceso ilícito a sistemas y equipos de informática del Código Penal Federal de México; se evaluaron cuáles son las disposiciones que a México le faltan por regular, para así mejorar su tipificación. Por último, también en este mismo capítulo se le dio tratamiento al tema de la cibercriminalidad y las Policías Cibernéticas en el aspecto internacional, y señalamos las recomendaciones emitidas por la ONU, en sus Congresos Internacionales sobre la Prevención del Delito y Justicia Penal.

Las conclusiones presentadas son de forma breve, clara, y concisa, enmarcadas ordenadamente en ocho numerales, cada una de ellas, alude a la problemática planteada en el cuerpo del trabajo, infiriendo en puntos que manifiestan ideas desarrolladas para dar respuesta a la condición que actualmente presenta el tema de investigación.

En la presente tesis se elaboró una propuesta legislativa debido a que la legislación mexicana lo requiere; en la que se contemplan los vacíos jurídicos y las omisiones legislativas que presenta el Código Penal Federal respecto a las conductas delictivas de los medios informáticos, la misma se encuentra en su respectiva sección, marcado con cursivas las disposiciones que se proponen.

La investigación realizada es de carácter cualitativa, por lo que se analizaron conceptos, definiciones, antecedentes históricos y la problemática que abunda en la tipificación del delito de Acceso ilícito a sistemas y equipos de informática en

México; por lo tanto se utilizaron diferentes tipos de métodos de investigación como los son: el método exegético para interpretar de forma literal, gramatical y lógica las legislaciones que tipifican este delito; también se utilizó el método deductivo para realizar un análisis practico valorando los elementos que conforma dicha legislación para inferir conclusiones; de la mano con el método deductivo se recurrió al método analítico con el objeto de examinar las normas que regulan este tipo de delito; además se aplicó el método histórico para conocer cuáles fueron las razones por las que México incorporó este delito al Código Penal Federal; y por último también se empleó el método comparativo para describir el marco jurídico que regula este delito en Alemania, Francia y España con México.

Las técnicas de investigación utilizadas fueron de carácter documental, de ellas se obtuvo la información necesaria para llevar a cabo la tesis, las mismas fueron recabas en las diferentes bibliotecas de la Universidad Autónoma de Sinaloa en los campus de Culiacán, Mazatlán y Los Mochis; en el Instituto de Investigaciones Jurídicas de la UNAM; así como también en los acervos jurídicos de la Universidad de Salamanca en España; además se consultaron fuentes formales de la ciencia jurídica como la Constitución Política de los Estados Unidos Mexicanos, el Código Penal Federal y los Códigos Penales de las entidades federativas de México; y en el ámbito internacional se consultaron el Código Penal de Alemania, el Código Penal de Francia y el Código Penal de España; de la misma forma se recurrió a hemerografía de revistas jurídicas y a sitios de la Internet oficiales, los que se encuentran descritos en el respectivo apartado de fuentes consultadas.

# CAPÍTULO PRIMERO

## INTERNET E INFORMÁTICA EN EL DELITO DE ACCESO ILICITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

La Internet es un sistema de información global; conecta a millones de personas en el mundo a su red de distribución. Bajo esta premisa afirmamos que dicha tecnología en la actualidad es una herramienta fundamental, utilizada con el contexto de propagar información mejorando el flujo de comunicación, sirviendo de auxiliar técnica en las labores de instituciones educativas, gubernamentales, científicas, empresariales y también para el ocio como uso personal.

Ciertamente sabemos las inmensidades de beneficios que nos ofrece la Internet, no obstante, esta misma también es el instrumento o medio utilizado para comisionar los llamados delitos informáticos o ciberdelitos, entre los cuales destaca el delito de Acceso ilícito a sistemas y equipos de informática, situando en un gran riesgo los bienes jurídicos tutelados de los usuarios de la red.

> De la misma manera, Suarez Mira afirma que la Internet ha supuesto una excepcional nueva vía de comisión de delitos, y no solo aquellos estrictamente vinculados a las tecnologías informáticas o cibernéticas, sino también de los que podríamos denominar como convencionales o tradicionales y que atentan en contra de bienes jurídicos como la libertad, la intimidad y el patrimonio[1].

Así pues, siguiendo con el criterio anterior, los delitos informáticos se encuentran inmersos y adheridos en la Internet, por lo tanto, debemos de ser cuidadosos y minuciosos al momento de navegar en la web para evitar ser una víctima más de la ciberdelincuencia.

[1] Suarez-Mira Rodríguez, Carlos, "Internet y derecho penal: viejos y nuevos delitos*",* en Fernández Rodríguez, José Julio y Sansó- Rubert Pascual, Daniel (eds.), *Internet: un nuevo horizonte para la seguridad y defensa,* España, Universidad de Santiago de Compostela, 2010, p. 105.

Por otra parte, la informática desempeña un rol fundamental en la comisión del delito de Acceso ilícito a sistemas y equipos de informática, pues ésta misma es el objeto material de dicho delito, y ante la falta de computadoras donde se mantenga resguardada información como datos informáticos sería difícil su configuración.

Para continuar con la descripción de este primer capítulo, se señalan algunos conceptos de la Internet, con el propósito de uniformar criterios de homologación y proporcionar el nuestro.

## I. INTERNET

### 1. *Concepto de internet*

Ahora bien, sin más preámbulo, le daremos tratamiento al concepto de la Internet que nos proporcionan diferentes autores especialistas en el campo de los sistemas de redes, con el objeto de que el tema sea más explícito, conciso y detallado, ya que, debido al popular empleo de la palabra, tiende a darse por conocida, y dejamos sin observación ciertos elementos importantes a saber.

> Huidobro Moya y Millán Tejedor, definen a Internet como una red de redes, (habitualmente se conoce como "la red"), con alcance mundial, en la cual se basan la gran mayoría de sistemas de información y comunicaciones actuales. Internet es una red abierta, independiente, funciona sobre la base de protocolo IP (Internet Protocolo), un estándar que permite la integración de voz, datos, música y video sobre una única infraestructura de red[2].

En esta conceptualización los coautores hacen mención, en destacar un elemento o característica fundamental de la Internet impregnado en su propia esencia, estamos hablando del carácter mundial, o bien, de su alcance global, que la convierte en el medio principal de la comunicación e información.

[2] Huidobro Moya, José Manuel y Millán Tejedor, Ramón Jesús, *Redes de datos y convergencia IP*, México, Alfaomega Grupo Editor, 2008, p. 87.

Luego entonces, Peter Kent nos dice que Internet es una enorme red de computadoras (la más grande del mundo) y está abierta al público… Lo que empezó como una herramienta del sector industrial y militar de Estados Unidos ahora está a disposición de cualquier persona[3].

Peter Kent nos señala otra característica que dota en el ser de la Internet, es la disponibilidad que tiene hacia todo el público, la red era exclusivamente un proyecto del gobierno de Estados Unidos en la década de 1960, (como veremos más adelante en el apartado de antecedentes de la Internet) más tarde fue evolucionando hasta perpetrar la exclusividad del gobierno, hasta convertirse a ser disponible para todas las personas.

Asimismo, López Angulo define a la Internet desde el ámbito de ser una red de redes, como un grupo de dos o más computadoras interconectadas para compartir información y recursos, a fin de estar en comunicación permanente con otros usuarios y equipos[4].

Al analizar los conceptos anteriores, podemos definir a la Internet como una enorme red de conexiones independientes conectada lógicamente a un sistema de información basado con el funcionamiento IP (Internet Protocolo), siendo de carácter mundial y abierta al público, que nos permite conectarnos con facilidad, de forma directa y rápida para comunicarnos cómodamente desde casa, escuela, oficina, y demás lugares públicos a los que se tenga acceso a la web.

De esta manera, como sabemos la red de Internet, está a la disponibilidad de las personas que cuenten con su acceso y con una computadora, o con los diferentes dispositivos electrónicos existentes, como por ejemplo laptops, Smartphones y tablets, que se conectan de forma inalámbrica a la red.

---

[3] Kent, Peter, *Serie ¡fácil! Internet*, 3a. ed., trad. Miguel Morales Carbajal, México, Prentice Hall Hispanoamericana, 1998, p. 3.

[4] López Angulo, Tania Clarisa et al., *Laboratorio de computo II,* 2a ed., México, Universidad Autónoma de Sinaloa, 2009*,* p. 45.

Por consiguiente, Internet nos ayuda a obtener información de diferentes tipos tanto educativa, médica, social, cultural, jurídica, económica, política, internacional, y una infinidad de temas de nuestro interés, a cerca de los cuales, podemos informarnos en tiempo real de las situaciones que pasan alrededor del mundo.

A su vez, Marquina Sánchez nos dice que:

> El mundo vive un proceso de globalización y desarrollo tecnológico nunca antes registrado. Desde las tres últimas décadas del siglo XX hasta nuestros días, el desarrollo de nuevas tecnologías de información y comunicación (TIC) ha suscitado una revolución tecnológica global que engendra cambios tecno-económicos en la sociedad post-internacional[5].

Por otro lado, con la evolución de la red en nuestros días, ha dado lugar a la creación de nuevos avances científicos, en laboratorios médicos, en instituciones educativas, en el Gobierno Federal y Estatal, y hasta se ha logrado un mayor flujo comercial conocido como comercio electrónico.

Debido al desarrollo tecnológico, económico, social y cultural que se ha presentado en México, se ha incrementado el uso de la Internet y la informática como parte de la vida cotidiana de las personas en la realización de diversas actividades, pero también, éstas, son las herramientas creadoras que dan múltiples facilidades para la comisión de ciberdelitos.

## 2. *Antecedentes de la Internet*

En este apartado se analizan los antecedentes de la Internet, los cuales son muy sencillos de explicar, pues no se remontan a la antigüedad, sino al contrario, ha sido un fenómeno relativamente nuevo, el cual se ha ido evolucionando hasta nuestros días, por lo que a partir del periodo de 1960 se empieza la conformación de la red.

[5]Marquina Sánchez, María de Lourdes, *Gobernanza global del comercio en internet,* México, UNAM, Instituto Nacional de Administración pública, 2012, p. 59.

Para llegar a ser el sistema de información que actualmente es, Internet se fue consolidando en distintas etapas, este proceso fue desarrollado y construido por diferentes colaboradores, cada uno de ellos aportó algo nuevo e innovador al proyecto de sistemas de redes, formándola cada vez más perfecta, ágil y audaz.

De esta manera, Peter Kent menciona que, Internet fue creada por el sector militar de Estados Unidos a fines del decenio de 1960, con el fin de que los investigadores del gobierno que trabajaban en proyectos militares pudieran compartir archivos de cómputo[6].

Conforme a la cita anterior, vemos que el proyecto de la Internet era de uso exclusivo del gobierno de Estados Unidos; se empezó con fines muy distintos a lo que actualmente es, tanto así, que el objetivo de la red no era ser de carácter público, sino cumplir con las necesidades militares del gobierno de Estados Unidos.

> Rojas Amandi expresa: un sistema tradicional de red con una computadora central les pareció muy vulnerable a los expertos del Ministerio de Defensa de Estados Unidos de América. Un ataque a una computadora central hubiese significado la caída de toda la red. Por eso, a partir de la década de 1960 empezó a desarrollarse un sistema de red que no dependiera de un servidor, sino que organizará de modo que cada computadora funcionara de manera independiente a otras[7].

La red fue desarrollada con la finalidad de que el equipo militar del Gobierno de Estados Unidos pudiera comunicarse de manera secreta, con el uso de computadoras y con un sistema de redes, para mantener una comunicación continua y de forma segura.

También notamos que desde el año antes citado, ya se preveía la posibilidad de que se pudiera efectuar algún delito informático a la computadora central del

[6] Kent, Peter, op. cit., p. 8.
[7] Rojas Amandi, Víctor, *El uso de internet en el derecho*, 2a. ed., México, Oxford, 2009, p. 2

gobierno de Estados Unidos, comisionado con las conductas de revelación de secretos, intromisión informática o un sabotaje informático.

Se avizoraba que algún experto en informática podía atacar a la red, al interceptar el sistema, con el propósito de estropear el flujo de comunicación, por lo tanto, se necesitaba que la red fuera invulnerable a un ataque que filtrara la información del organismo gubernamental.

En 1965, Lawrence Roberts conectó una computadora TX2 en Massachusetts con un Q-32 en California a través de una línea telefónica conmutada de baja velocidad, creando así la primera (aunque reducida) red de computadoras de área amplia jamás construida[8].

De esta manera, el desarrollo de la Internet iba formándose a pasos agigantados, pues el proyecto de la red cada día se convertía en más completo, pero aun así faltaba que la información transportada por la red fuera más rápida, segura y eficaz.

Los coautores Huidobro y Millán, refieren:

> Hasta 1969 se pone en marcha una red experimental que hizo posible el intercambio de información entre dos o más ordenadores. A esta red se le llamó ARPANET, y es considerada como el embrión de lo que con los años ha llegado a ser Internet. ARPANET nació en los años de la "guerra fría". Ante estas perspectivas los servicios de inteligencia se plantearon la necesidad de estar comunicados con el temor de que existiera un ataque nuclear. La idea era conseguir una red de tecnología tal que asegurase que la información llegará al destino aunque parte de la red quedara destruida[9].

Lo que hoy conocemos como la Internet, fue una evolución del sistema ARPANET (*Avanced Research Projet Agency Network*) es decir, Agencia de Proyectos de Investigación Avanzada, la cual, tenía la finalidad de intercambiar

[8] López Angulo, Tania Clarisa et al., *op. cit.,* p.63
[9] Huidobro Moya, José Manuel y Millán Tejedor, Ramón Jesús, *op. cit.,* pp. 87 y 88.

información y mantener la comunicación que le fuera conveniente al Gobierno de Estados Unidos.

Por lo tanto, ante la situación que se vivía por la guerra fría, Estados Unidos buscaba ser precavido, de esta manera, empezó a crear dicho proyecto de defensa de tecnología militar para asegurar las comunicaciones ante un ataque a la red o alguno de tipo nuclear, examinando las medidas necesarias que considerara pertinente.

Así pues, ante el riesgo probable de un ataque nuclear, Estados Unidos innovaba y perfeccionaba cada vez más el proyecto militar de la Internet, con el propósito de mantenerse en comunicación constante, y que esa información fuera capaz de transportarse, sin pensar aún en que dicha red se convertiría de gran utilidad.

Para el funcionamiento de ARPANET fue necesario construir procesadores especiales, a los que se les denominó procesadores de mensajes de interfaz (IMP). El primer procesador de este tipo fue puesto en funcionamiento el 1 de agosto de 1969 en la Universidad de California en Los Ángeles (UCLA)[10].

En palabras más comunes, podemos explicar que el funcionamiento de ARPANET consistía en mandar mensajes, con la ayuda del nuevo sistema de redes IMP, éste dividía el mensaje en partes pequeñas para que pudiera tomar rutas diferentes, y después, ya que llegara a su destino, se convertía en el mensaje original, con el objetivo de que la información no fuera interceptada o atacada por algún experto destruyéndola o modificándola.

A principios de la década de 1980 Internet se separó de ARPANET, de tal forma que se desligó de los objetivos militares y se expandió de una manera más rápida, esto permitió que instituciones científicas tanto estadounidenses como extranjeras se enlazaran a Internet[11].

[10] Rojas Amandi, Víctor, *op. cit.,* p. 2.
[11] *Ibidem,* p. 3.

Asimismo, durante éste periodo las instituciones científicas de Estados Unidos crean otras redes, debido a que tenían la necesidad de conectar información, compartir conocimiento y colaborar en proyectos de investigación, de esta manera, Internet se separa de ARPANET, permitiendo a instituciones científicas y educativas la conexión al sistema de información. ARPANET cambia su objetivo meramente militar para ofrecer intercambio de información y comunicación de índole académica y científica.

Después de este periodo, Joyanes refiere que en 1983, nació la Internet como red de interconexión entre ARPANET, CSNET y MILNET (red desencajada de ARPANET, con fines militares), unidas todas con protocolos TCP/IP y las que se irían añadiendo posteriormente otras redes de Estados Unidos y de otros países[12].

Por lo tanto, podemos observar que luego de veintitrés años, la red se independizó de otras redes, y se le empezó a llamar como hoy lo conocemos: la Internet, de esta manera, se fue extendiendo fuera de Estados Unidos hacia otros países del mundo, ahora no con el propósito militar, sino con el propósito de proporcionar información y comunicación a los usuarios.

> En 1986 se fundó la *National Science Fundation Network* (Fundación Nacional para la Ciencia) (NSFNET). Financiada por el Gobierno federal estadounidense, la NSFNET creó diferentes líneas de enlace para Internet, a las que se denominó *backbones* (espina dorsal), con las que se facilitaba la transferencia de datos. A partir de entonces, Internet inició su expansión hacia el exterior de Estados Unidos de América, sobre todo hacia Europa[13].

Luego de este periodo, se buscaba que la red de internet fuera más rápida, por lo que, se fundó la NSFNET, un nuevo sistema permitía la transferencia de datos con la ayuda de líneas de enlaces de alta velocidad, así la Internet expandió sus redes por todo Estados Unidos llegando hasta el continente Europeo.

---

[12] Joyanes, Luis, *op. cit.,* p. 103.
[13] Rojas Amandi, Víctor, *op. cit.,* p. 3.

> Con base a lo anterior, Fernando Rodríguez apunta que México fue el primer país de la América hispana en conectarse a la red en 1989 (España lo hizo en 1990). Los primeros sitios mexicanos fueron de índole académica y se encontraban en el Instituto Politécnico Nacional, el Instituto Tecnológico de Estudios Superiores de Monterrey, la Universidad de las Américas (Puebla), la Universidad de Guadalajara y la Universidad Nacional Autónoma de México[14].

Las universidades de México, al igual que las universidades de Estados Unidos, se conectaron a la Internet para fines académicos, con el propósito de comunicarse entre sí y desarrollar nuevos avances de tecnología y ciencia, aprovechando el nuevo sistema de alta velocidad, lo que trajo consigo nuevas oportunidades de crecimiento en el ámbito educativo y científico, tanto para alumnos, profesionistas y para docentes.

> Por su parte, Anibal Pardini expresa que la red de WWW (World Wide Web) se inició en marzo de 1989, cuando Tim Berners-Lee, del laboratorio de física del Consejo de Investigadores Europeos *(Conseil Européen pour la Recherche Nucleaire*: CERN), propuso el proyecto como un medio para comunicar mejor los propósitos de investigación entre los miembros de la organización[15].

Por lo tanto, desde el año de 1969 hasta 1989 podemos observar la evolución que ha tenido la Internet, al incorporar su primer navegador como parte del *software* de la computadora, con lo cual se permite acceder al mundo virtual, para navegar en la red y páginas de la Internet, buscar información, reproducirla tanto en video como en sonido. Sin duda, en esos veinte años se presenta un gran cambio tecnológico al crearse la WWW.

---

[14] Fernández Rodríguez, José Julio, *Lo público y lo privado en internet, intimidad y libertad de expresión en la red*, México, UNAM, Instituto de investigaciones jurídicas, 2004, p. 8.
[15] Pardini, Anibal A., *Derecho de internet*, Argentina, Ediciones La Roca, 2002, p.52.

WWW es un navegador web, que permite recuperar y visualizar documentos, desde servidores web de todo el mundo a través de internet. Cualquier navegador actual permite mostrar o ejecutar gráficos, secuencias de video, sonido animaciones y programas diversos[16].

De este modo, Tim Berners-Lee con su idea nos abrió las puertas para navegar en el ciberespacio conocido como la Internet, de manera automática y rápida, con la finalidad de realizarse el intercambio global de la información y del conocimiento.

La web fue creada con una cierta filosofía, una posición de principios frente a los desarrollos que se venían dando en materia de publicaciones, de desarrollo de software, de derechos de autor y de difusión. Esta filosofía puede resumirse en tres principios: todos pueden publicar, todos pueden leer, nadie debe restringir[17].

Así podemos ver que los principios de la web rigen en la actualidad, ya que todos podemos publicar en la web (publicar información, publicidad y/o videos); todos podemos leer (información, libros, imágenes y demás documentos que se prefieran); y nadie debe restringir (escatimar información o flujo de comunicación).

> Hasta 1995 la NSFNET intentó interponer una política de uso aceptable (*aceptable use policy),* con el fin de que Internet se utilizará sólo con propósitos científicos, no comerciales. Sin embargo dicha política fue puesta en vigor a principios de 1995, cuando el Gobierno estadounidense decidió privatizar y no otorgar más subsidios a Internet. Desde ese año es posible utilizar este sistema para objetivos de índole muy diversa, incluidos los de carácter comercial[18].

En el año de 1995 hubo un cambio drástico para la historia de la Internet, pues, el Gobierno de Estados Unidos autoriza que la red sea utilizada para fines

[16]López Angulo, Tania Clarisa et al., *op. cit.,* p. 66.
[17] Centro de Investigación de la Web, *Cómo funciona la web,* Chile, Universidad de Chile, 2008, p.14.
[18] Rojas Amandi, Víctor, *op. cit.,* p. 3.

académicos y comerciales, como la conocemos hoy en día, en la que miles de empresas se conectan a la red para comercializar sus productos o servicios.

Una vez que la Internet se extendió internacionalmente, se hizo crear nuevos dominios de nivel superior que fueran más específicos. Para satisfacer esta necesidad, se desarrolló un nuevo sistema de dominios geográficos, en el que una abreviatura de dos letras representa a un país[19].

Por ejemplo, el dominio que le corresponde a México es el enmarcado con: .mx, por eso las mayorías de páginas web que consultamos terminan en .com.mx para comercios mexicanos; .edu.mx instituciones educativas mexicanas; .gob.mx para el gobierno mexicano; y .org.mx organizaciones no lucrativas mexicanas.

Posteriormente, el 24 de octubre de 1995, el FNC (*Federal Networking Council,* Consejo Federal de la Red) aceptó unánimemente una resolución definiendo el término Internet. La definición se elaboró de acuerdo con personas de las áreas de Internet y derechos de propiedad intelectual[20].

Al analizar los antecedentes de la Internet, podemos apreciar que transcurrieron treintaicinco años desde su creación para que se le otorgara el nombre que actualmente posee ante derechos de propiedad intelectual, asentado todo lo anterior en Estados Unidos como su país de origen, por lo que el nombre de Internet proviene del inglés que significa *International Netword.*

Y bien, para concluir, con este apartado de antecedentes, podemos decir que la Internet, ha tenido un gran desarrollo tecnológico, ya que con sólo siete lustros de haber nacido con propósitos militares, se fue incorporando para brindar apoyo a instituciones científicas y educativas, para con posterioridad ingresar al ámbito comercial, y finalmente, lo que hoy lo conocemos como de uso personal para comunicarnos, buscar información y entretenimiento a millones de personas.

---

[19]Hahn, Harley, *Internet manual de referencia*, 2a ed., trad. de José Pieltain Álvarez Arenas, España, McGraw-Hill de España, 1997, p. 79.
[20] Huidobro Moya, José Manuel y Millán Tejedor, Ramón Jesús, *op. cit.,* p. 88.

Actualmente la red es utilizada en los bancos, empresas, tiendas de autoservicio, en instituciones sociales, en el Gobierno, e inclusive también en el hogar para el uso personal; la misma, ha transformado el manejo de operatividad brindando más facilidad a las funciones que se desempeñan en diversos oficios y logrando mayores relaciones comerciales.

3. *El derecho de acceso a Internet en México como un Derecho Humano*

Internet tiene su red en todo el mundo, actualmente en México su popularidad es muy grande, tanto para personas menores como para mayores de edad, son miles los mexicanos que usan la red diariamente, para realizar diferentes actividades en su vida personal o profesional.

El acceso a Internet juega un rol muy importante en la expansión de las TIC (Tecnologías de la Comunicación y la Información), y los datos recientes sugieren que la computadora e internet han dejado de ser obligaciones o herramientas escolares y laborales para incorporarse al hogar[21].

En el sentido que expresa Téllez Carvajal, de que la Internet ha dejado de ser una obligación en las actividades de escuela y trabajo para inmiscuirse en el hogar, consideramos este postulado como cierto; hoy en día podemos observar que la red se ha convertido en una herramienta muy útil para realizar diferentes fines y más que un lujo es una necesidad para todos.

Así pues, bajo la premisa anterior, Internet se ha vuelto tan necesaria en nuestras vidas, tanto así que el acceso a esta misma se ha convertido en derecho humano contemplado en la Constitución Política de los Estados Unidos (C.P.E.U.M.).

Del análisis al artículo 1° de la C.P.E.U.M. en el último párrafo (fecha de última reforma publicada en el D.O.F el 15 de mayo de 2019), hemos de reconocer es un Derecho Humano que todas las personas puedan gozar de la Internet, sin

[21] Téllez Carvajal, Evelyn (coord.), Derecho y TIC. Vertientes actuales, México, UNAM, Instituto de Investigaciones Jurídicas, 2016, p. 18.

importar su origen étnico o nacional, el género, la edad, las discapacidades, la condición sexual, las condiciones de salud, la religión, las opiniones, las preferencias sexuales o el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto menoscabar los derechos y libertades de las personas

> Entre tanto, Díaz Revorio precisa: el 1 de junio de 2011 el Relator Especial de la Organización de las Naciones Unidas (ONU) para la Libertad de Opinión y Expresión se emitió una Declaratoria sobre Libertad de Expresión e Internet. En dicha Declaración se conceptualiza el derecho de acceso a Internet como un derecho humano y se insta a los Estados a promover el acceso universal a Internet para garantizar el disfrute a la educación, la atención, a la salud, y el trabajo, el derecho de reunión y asociación así como a elecciones libres[22].

Por ende, el Derecho de acceso a Internet como Derecho Humano comienza con base a este Decreto emitido por la ONU, al expresar que todas las personas tienen el derecho del uso, goce y disfrute de la red, como parte de su libertad de expresión y libertad de opinión.

Con ello, la ONU insta a sus Estados Miembros a legislar el Derecho de acceso a Internet, por lo que los Estados deben no sólo legislar el acceso a Internet como derecho, sino también proporcionar los medios necesarios para que los mexicanos puedan hacer uso del mismo.

Conforme a esta recomendación de la ONU, México ha establecido el Derecho de acceso a Internet regulado por la Constitución Política de los Estados Unidos Mexicanos en el titulo primero denominado de los Derechos Humanos y sus garantías, en el artículo 6° párrafo tercero se establece:

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

[22] Díaz Revorio, Francisco Javier, Los derechos humanos ante los nuevos avances científicos y tecnológicos, México-España, Tirant Lo Blanch, 2009, p. 3

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

Este párrafo fue agregado a la C.P.E.U.M el 11 de junio de 2013, por el decreto D.O.F: 11/06/2013, publicado en el Diario Oficial de la Federación, el cual, entró en vigor al día siguiente de su publicación, y hasta la fecha no ha sido reformado.

Como podemos observar México no tardó demasiado tiempo en regular la petición hecha por la ONU, a partir de entonces el Gobierno mexicano ha prometido garantizar el acceso a Internet en el territorio, sin embargo, en la realidad en muchas ciudades y comunidades del Estado mexicano el acceso a la red está fuera del alcance de las personas.

En la República Mexicana el acceso a Internet se ha expandido de forma significativa, creando de esta manera que muchos mexicanos tengan conexión la red ya sea por medio de contrato con uno de los proveedores de servicios de acceso a Internet en el hogar u oficina, o bien, por medio de Internet gratuito por parte del Gobierno, o por algún cibercafé.

Con base a este decreto, y para hacer efectivo este Derecho, el Estado mexicano inició el proyecto México Conectado, con el propósito de garantizar el Derecho Constitucional de acceso a Internet de banda ancha plasmado en el artículo 6° de la C.P.E.U.M[23].

Con este proyecto, el Gobierno de México crea el sistema de redes de Internet gratuito denominado: México Conectado, instalado en sitios públicos para promover el servicio de Internet en escuelas, universidades, bibliotecas, parques, plazuelas, museos, canchas deportivas, centros de salud, centros de recreación, clínicas de salud, H. Ayuntamientos y oficinas de Gobierno.

[23] https://mexicoconectado.gob.mx/?page_id=10572

Asimismo, por medio del proyecto México Conectado más mexicanos tienen acceso a Internet de banda ancha gratuito en sitios públicos, donde pueden disponer de este recurso por medio de vía inalámbrica de WI-FI (*Wireless Fidelity*), es decir, fidelidad sin cables o inalámbrica, desde diversos dispositivos electrónicos.

De acuerdo con el documento Lineamientos del Proyecto México Conectado nos dice que:

> El objetivo del proyecto es establecer las políticas, mecanismos y acciones necesarios para brindar acceso a la banda ancha en todos los sitios públicos del país, en el contexto de una red troncal y una red compartida de Telecomunicaciones, a través de un esfuerzo coordinado por el Gobierno Federal con la participación de los Poderes Legislativo y Judicial de la Unión, los Poderes de los Estados de la Federación, los municipios, los órganos de gobierno del Distrito Federal, órganos públicos autónomos, dependencias y entidades políticas de los tres órdenes de gobierno, instituciones académicas, organizaciones de la sociedad civil, y los demás entes que, por razones de interés general, determine la Secretaria de Comunicaciones y Transporte[24].

Como ya vimos el Estado nos ofrece el acceso a Internet gratuito en sitios públicos, empero, esta red suele ser muy lenta debido a que muchas personas se encuentran conectadas a la vez; de este modo, es de más practicidad conectarnos a Internet desde el hogar.

Conforme a la estadística del INEGI denominada Estadística a propósito del día mundial del internet (17 de mayo), nos dice que, al segundo trimestre de 2016, el 59.5% de la población se declaró usuaria de Internet, y 47% de los hogares del país tienen conexión a la web[25].

---

[24] *Lineamientos del proyecto México conectado,* secretaría de comunicaciones y transportes, México 2013, p.5, *http://mexicoconectado.gob.mx/images/archivos/2013_09_27_Lineamientos_Mexico_Conectado.pdf.*

[25] Instituto Nacional de Estadística y Geografía INEGI, *Estadística a propósito del día mundial del internet*, México, mayo 2017, p.1.

De la anterior estadística realizada en el año de 2016 y publicada en el año de 2017, podemos afirmar que casi la mitad de los hogares mexicanos cuentan con acceso a la red desde su casa, y el otro 12.5% de la población son usuarios de Internet quienes buscan la conexión por otros medios.

> Por otra parte, la más reciente encuesta realizada por el INEGI en el segundo trimestre del año de 2018 y publicada con fecha de 2 de abril de 2019, denominada Encuesta Nacional Sobre la Disponibilidad y Uso de las TIC en los Hogares 2018 (ENDUTIH 2018), determina que los hogares con acceso a la Internet en México en el año de 2017 fueron de 50.9% de la población; para el año de 2018 se muestra un incremento a 52.9% de la población, siendo esta cifra equivalente a 18.3 millones de hogares los que cuentan con acceso a la red en México; 73.1% de la población urbana es usuaria de este servicio y el 40% de la población es de zonas rurales[26].

Conforme a la Encuesta anterior de 2018, podemos apreciar que año con año van incrementando los usuarios de la Internet en México, asimismo, se aprecia que son millones los hogares en México que tienen el acceso a este servicio debido a los beneficios que ofrece la red.

Los estados que más sobresalen por la mayor proporción de usuarios de la Internet son: Sonora, Baja California, Quintana Roo, Nuevo León, Baja California Sur, Sinaloa, Chihuahua y Cuidad de México; mientras los que los estados con menos usuarios son Chiapas y en último lugar Oaxaca[27].

Así podemos ver que en México los usuarios de la Internet se conectan con mayor número en zonas urbanas, mientras que en las zonas rurales son menos las personas son usuarias de la red, por lo que apreciamos que en unas entidades federativas hay más facilidades al acceso a la Internet.

---

[26] Instituto Nacional de Estadística y Geografía INEGI, *Encuesta Nacional Sobre la Disponibilidad y Uso de las TIC en los Hogares 2018 (ENDUTIH 2018),* México, abril 2019, pp. 1, 10 y 19.
[27] *Ibidem,* p. 6

Por ello, para tener acceso a Internet desde el hogar, nos es posible contratar la conexión con los distintos proveedores de servicios de Internet, estos nos ofrecen el servicio por un módico pago al mes, no obstante, muchos hogares no pueden costear el servicio de la red.

Para esto, el Estado establece la libre competencia de proveedores de servicios de Internet, con ésta, se ha logrado que compañías ofrezcan el servicio a un precio justo, de esta manera, se ha incrementado que más hogares y empresas cuenten con la red, contratándola con el proveedor de su interés.

Lo antes precisado se refleja en el artículo 28 de la C.P.E.U.M el que señala:

En los Estados Unidos Mexicanos quedan prohibidos los monopolios, las prácticas monopólicas, los estancos y las exenciones de impuestos en los términos y condiciones que fijan las leyes. El mismo tratamiento se dará a las prohibiciones a título de protección a la industria.

Así pues, como refiere el artículo anterior las prácticas monopólicas en México se encuentran prohibidas, por lo cual, son múltiples las empresas que nos puedan brindar el acceso a Internet, de igual forma a como lo ofrecen otras que se dediquen al mismo ramo comercial.

Por ende, un proveedor de acceso, es un intermediario que facilita el acceso a internet a las personas o empresas interesadas. Los proveedores de acceso suelen ofrecer a sus clientes la posibilidad de acceder a internet por cualquiera de los sistemas siguientes: baja velocidad y alta velocidad[28].

Está a nuestro albedrio, contratar el paquete de Internet que nos convenga, ya sea con baja velocidad o el de alta velocidad, y con el proveedor de servicios que nos beneficie, ya que estos, tienen diferentes costes algunos más elevados que otros, dependiendo de sus políticas de oferta y demanda.

[28] Carballar, José A., *Wi-Fi instalación, seguridad y aplicaciones,* México, Alfaomega Grupo Editor, 2007, p. 147.

Para lograr tener acceso a Internet en la computadora o con los diferentes dispositivos electrónicos deben estar conectados a la red, hay varias formas de conexión a Internet, las pueden ser por medio de modem por servicio de cable, o por satélite, todas ofrecen el mismo servicio de Internet pero con distintas formas de conexión.

Estabrook dice que un modem es un dispositivo electrónico que convierte los datos de la computadora en señales de audio. Estas señales pueden ser transmitidas por una línea telefónica común. Al otro extremo de la línea, otro modem reconvierte las señales de audio en datos de computadora[29].

La puerta del acceso a Internet son los modem, con su tecnología innovadora nos ofrecen conexión a la red de alta velocidad, con el servicio ilimitado e inalámbrico, y a la vez, son fáciles de instalar, los cuales, los podemos tener en diversos sitios como en la casa, oficina, escuela, entre otros.

> Kathy Ivens señala que el modem telefónico se conecta a Internet a través de la red telefónica básica (RTB), que comparte con el teléfono y el fax. La RTB es una red analógica y la máxima velocidad que puede lograr es de 56 Kbps (Kilobits de datos por segundo). A este acceso se le denomina conexión de acceso telefónico[30].

El servicio de Internet de conexión por RTB ofrecía a los usuarios el enlace a la red con baja velocidad, era tan mínima la velocidad de la Internet que se renovaron a los módems electrónicos, los que actualmente conocemos, y que brindan mayor velocidad, por lo que el servicio de modem telefónico quedó obsoleto, porque no se podía utilizar la red y el teléfono al mismo tiempo.

Por otra parte, el modem cable es un dispositivo, un modem, que permite el acceso a alta velocidad a través de las redes de televisión por cable. El sistema

---

[29] Estabrook, Noel y Bill, Vernon, *Aprendiendo Internet en 24 horas*, trad. de Ricardo de la Barrera Ugalde, Estados Unidos, Prentice-Hall Hispanoamericana, 1997, p. 40.
[30] Ivens, Kathy, *Internet en casa,* trad. de Luiciano García Tosina, España, McGraw-Hill Interamericana de España, 2004, p. 14.

permite velocidades de hasta 40 Mbps, aunque por razones técnicas y comerciales, los proveedores suelen limitar este acceso a bastantes inferiores[31].

Las compañías que ofrecen el acceso a Internet por cable, dan un buen servicio, pues los canales de televisión no se ven dañados con el uso de la red, la velocidad es muy rápida, y también se obtiene el servicio de Internet inalámbrico de varios metros, así se puede disfrutar del acceso a la web sin estar cerca de modem, lo que nos permite a la vez realizar otras actividades.

Si se vive en un lugar remoto donde no existe servicio de telefonía fija o de televisión por cable pero se necesita conexión a internet a alta velocidad, la solución apropiada es la conexión por satélite. La conexión por satélite sólo necesita tener una vista despejada al cielo del sur[32].

La conexión por satélite es excelente para aquellos lugares alejados de la ciudad o zonas rurales, donde se necesita del acceso a Internet, con esta tecnología muchas personas que viven en este tipo de lugares se pueden conectar a la red y recibir sus beneficios de comunicación e información, sin importar la lejanía en la que se encuentren.

No obstante, los usuarios de la web que no tienen la posibilidad contratar el servicio de Internet con algún proveedor en su casa, o bien, que no tengan la manera de trasladarse a un sitio público donde se encuentre el acceso a la red gratuita, buscan la conexión por medio de cibercafés.

Ruelas Ana Luz nos dice que el cibercafé es el centro de acceso público a las TIC que predomina en el mundo por su versatilidad, pues ofrecen una variedad de servicios de telecomunicaciones: llamadas telefonías locales y de larga distancia, acceso a internet y cómputo[33].

---

[31] Carballar, José A., *Wi-Fi instalación, seguridad y aplicaciones, op. cit.,* p. 151.
[32] Ibídem, p. 153.
[33] Ruelas, Ana Luz, *Internet y los accesos públicos: cibercafés en Sinaloa,* México, Universidad Autónoma de Sinaloa, 2012, p. 97.

Este tipo de negocios se han expandido de forma muy numerosa en el país, ofrecen la renta de una computadora con acceso Internet a bajo costo por tiempo determinado, con lo cual, benefician a muchas personas, los cibercafés también son llamados ciber Internet, o solamente ciber, en algunos, aparte de tener el servicio de acceso a la red, también tienen el servicio de restaurante o cafetería.

Asimismo, afirma Ruelas Ana Luz que los ciber son más comunes en naciones donde el índice de Internet en los hogares es bajo, en los países con alta conectividad proliferan para dar el servicio a turistas o viajeros y a personas que trabajan lejos de sus hogares[34].

Algunos cibercafés son exclusivamente dedicados a brindar acceso a Internet para usos académicos su lugar es tranquilo y callado como el de una biblioteca, mientras que otros son para usos de juegos en línea con computadoras y artículos de cómputo especiales para dichos juegos.

En el mismo sentido, aunque el cibercafé es un sitio reducido, ahí mismo se puede imprimir archivos, sacar copias, escanear documentos y adquirir productos de papelería, lo que se suma a esto un gran beneficio a los usuarios, pues cuenta con varios servicios a la vez.

Hoy en día el acceso a Internet es tan amplio que lo podemos tener no sólo en la computadora de escritorio, sino también en diferentes dispositivos electrónicos como laptops, celulares (smartphones), tabletas electrónicas, consolas de videojuegos, y las nuevas televisiones llamadas smart-tv.

Estos dispositivos los conectamos a Internet por medio de conexión inalámbrica, permitiéndonos conectarnos a la red sin la necesidad de cables a módems, haciendo más práctica, fácil y rápida la conexión desde cualquier lugar donde se encuentre la red.

[34] *Ibídem,* p. 98.

Con las formas de conexión anteriormente señaladas (por modem, satelital o inalámbrica), es más fácil obtener el acceso a Internet, asimismo, la red se ha expandido por todo el territorio mexicano, considerándose una fuente de vital importancia en la comunicación, información y educación de las personas.

Así pues, el uso de la red en México es muy grande lo que conlleva a que el país se desarrolle tanto económica como socialmente, de esta manera también el campo científico y tecnológico se ve beneficiado al tener esta herramienta de gran ayuda en sus actividades, por ende reprimir el acceso a Internet seria como cerrarle las puertas al cambio, a la educación, arte, distracción, ciencia, comunicación, y al mundo entero.

4. *Usos de la Internet en el derecho*

La Internet se ha convertido en una herramienta fundamental en el campo del derecho (en cualquiera de sus disciplinas) utilizada por ministros, magistrados, jueces, legisladores, abogados, notarios, servidores públicos, docentes, estudiantes del derecho, y demás personas que se encuentren inmersas en el campo jurídico.

Es grande el beneficio que aporta la Internet hacia las tareas del derecho, pues nos ayuda a buscar y compartir información, a comunicarnos constantemente por correo electrónico o por videoconferencia con colegas y estudiantes, a comprar en línea, y también se usa este recurso, como medio publicitario para muchos despachos jurídicos, notarias y para el sector gubernamental.

Si bien decimos que la red nos ofrece muchos beneficios, el más importante para el campo del derecho, es el de buscar información jurídica, y sin duda la red nos hace más fácil la tarea, al tener buscadores de páginas web, sin ellos tardaríamos mucho tiempo en encontrar la información en todo el cúmulo de páginas web existentes.

Asimismo, López Angulo refiere que los motores de búsqueda son sistemas que buscan en internet cuando les pedimos información sobre algún tema. Las

búsquedas se hacen con palabras clave o con árboles jerárquicos por temas; el resultado de la búsqueda es un listado de direcciones web[35].

Los buscadores que más utilizamos son Google, Yahoo! search, Internet Explorer, Bing, Mozilla, ASK, Microsoft, Noxtroum, dmoz, entre otros, estos buscan la página web por medio de palabras claves y en pocos segundos dan por resultado una lista a las que podemos acceder una y otra vez.

Por consiguiente, otra de las tareas elementales de los profesionistas del derecho es buscar jurisprudencias y tesis aisladas, pues estas son de gran importancia para el actuar del derecho, y por medio del buscador es más sencillo al incorporamos al sitio web de la Suprema Corte de Justicia de la Nación y empezar con la búsqueda.

Aunado a los demás, otro de los usos que el profesionista del derecho le da la red es la búsqueda de documentos en materia legislativa, estos los podemos encontrar en las páginas web oficiales del Gobierno Mexicano, estas páginas son: la de la Cámara de Diputados y Senadores, el Diario Oficial de la Federación, la Suprema Corte de Justicia de la Nación y demás páginas de secretarías y organismos gubernamentales y autónomos.

Del mismo sentido, la información en materia legislativa es tan importante para los juristas, como también, la información del Derecho Internacional Público, con los Tratados Internacionales ratificados por el Senado de la Republica, pactos de los que el Estado mexicano sea parte, leyes internacionales y los diferentes organismos internacionales, y sin duda el internet nos facilita la obtención de esta información.

Asimismo, el profesionista del derecho puede encontrar en la Internet, libros en formato PDF y revistas jurídicas, sirviendo como instrumentos de consulta los cuales se en este formato para ser descargados, evitándonos el traslado y el coste de ir a las librerías a comprarlos en físico.

[35] López Angulo, Tania Clarisa et al., *op. cit.,* p. 78.

Igualmente, un uso más que la Internet le ofrece al campo del derecho es poder acceder a bibliotecas virtuales de diferentes universidades y consultar los libros completos en línea, así como también ver su cita bibliográfica, esto es de gran ayuda principalmente para estudiantes, docentes e investigadores del derecho, pues la consulta de libros es su fuente principal de conocimiento.

Con este beneficio, se evita el desplazamiento a la biblioteca o tiendas, en búsqueda de información documental jurídica, e inclusive en la red se pueden encontrar los libros con las actualizaciones más recientes, o bien, si no encontramos el libro en línea para poderlo descargar o consultar, podemos ver que librería lo tiene en físico, para ir a comprarlo con mayor precisión y ahorrar tiempo o en su defecto realizar la compra por la web.

Por otra parte, para el profesionista en derecho es importante estar comunicados, por ello, el correo electrónico es un servicio que presta la red, permite enviar y recibir mensajes a uno o varios destinatarios a la vez. Con el correo electrónico (también llamado e-mail) sabemos quién nos manda un mensaje con sólo ver el nombre de la dirección del correo, podemos enviar y recibir no sólo mensajes, sino también archivos, documentos, imágenes y videos, a otros usuarios sin importar el lugar donde se encuentren.

Otra forma de comunicación que nos ofrece la Internet, lo es la videoconferencia, ésta herramienta es fundamental para los directivos del Gobierno, abogados, profesores del derecho, entre otros más, con ésta función se pueden tratar y resolver problemas de urgencia y de forma inmediata.

Luque Ordoñez nos dice que, la videoconferencia se define, de manera genérica como la tecnología que permite la comunicación simultánea entre dos o más interlocutores geográficamente dispersos mediante el intercambio de audio, videos y datos[36].

[36] Luque Ordoñez, Javier, *Videoconferencia tecnología, sistemas y aplicaciones,* México, Alfaomega Grupo Editor, 2009, p. 2.

Con la videoconferencia se ahorra tiempo, dinero y esfuerzo; se evitan los traslados al llevar a cabo una reunión en otro lugar, de esta forma se incrementa la comunicación, y se aumenta la productividad, pues en instantes nos podemos comunicar con las personas sin salir de la oficina, despacho o domicilio personal.

La red también pone a disposición del profesionista del derecho la opción de comprar en línea, esta es una gran ventaja debido a que si en la librería no encontramos el libro que estamos buscando, lo podemos encontrar en las tiendas online, y en ocasiones el precio puede ser aún más bajo.

> De esta manera, Kathy Ivens nos dice que, el termino compra segura cobra un significado singular cuando se trata de compras online, supone asegurar que su información personal nunca se usa sin su conocimiento y sin su consentimiento. En efecto, la popularidad de la web ha provocado la aparición de un nuevo tipo de tiendas, los comercios online. El más famoso de todos ellos es, con diferencia, Amazon.com, Amazon empezó como una librería online pero se ha convertido en unos grandes almacenes online que venden una amplia gama de productos[37].

Hay muchas tiendas online en la red, de las cuales el profesionista del derecho puede usar para poder comprar, sin moverse de su despacho a hacer la compra en físico, de la misma manera, la compra hecha llegará en un paquete a la dirección que más le sea conveniente, de esta forma se ahorra tiempo.

Por otro lado, para los abogados y notarios que ofrecen sus servicios hacia la comunidad, la publicidad en Internet es otra herramienta que está al día, ésta, es una nueva forma de darse a conocer promocionando su despacho y servicios en la web para encontrar nuevos clientes.

Del águila nos dice que, la publicidad en Internet es una extensión de la radiodifusión o la televisión, en este caso, el medio es un *website* que provee

[37] Ivens, Kathy, *op. cit.,* p. 147 y 148.

contenidos, de pago, o no, servicios asociados, y mensajes publicitarios en forma de *banner.* La audiencia de este tipo de web es masiva o muy especializada[38].

Promocionarse en la web es muy sencillo, se puede hacer por medio de la creación una página web, o bien, que la publicidad digital está inmersa en otras páginas web, para esto, se tiene que contratar a una persona especialista en diseño de páginas web.

Son millones los internautas que se conectan a la red al día, encontrando publicidad en la mayoría de páginas web, la publicidad web está marcando un nuevo paradigma en los negocios, esto quiere decir que los despachos que cuentan con este servicio están más actualizados que otros, al incorporarse en la web.

La publicidad, es la puerta de entrada de los clientes al negocio, es la estructura que le informa al cliente los servicios que se prestan, y si se publica en los sitios web, y los despachos de abogados o notarios están aprovechando este recurso para generar más clientes.

Ahora bien, retomando los puntos anteriores podemos asumir la postura de que la Internet ofrece gran variedad de beneficios a los profesionistas del derecho, eso sin duda alguna, asimismo no se debe de dejar al lado la seguridad de los sistemas informáticos para evitar algún ciberdelito.

5. *La Internet y el ciberdelito*

> Las redes y los sistemas de información y telecomunicaciones, han generado nuevos modelos de negocio, difuminando las fronteras, haciendo participes a los ciudadanos de una globalización desconocida hasta hace muy pocos años. Nos encontramos ante una nueva revolución industrial basada en la digitalización de la información[39].

---

[38] Águila, Ana Rosa del, *Comercio electrónico y estrategia empresarial: Hacia la economía digital,* 2a ed., España, Alfaomega Grupo Editor, 2001, p. 139.

[39] Briera Dalmau, Carme, "La ciberseguridad: consideraciones y apuntes sobre el régimen jurídico aplicable a la seguridad de las redes y sistemas de la información", en Escudero Gallego, Román y Martínez Garrido Santiago (Dirs.), *Cuadernos de derecho para ingenieros, ciberseguridad,* España, Wolters Kluwer España, 2017, p. 271.

Como manifiesta Briera Dalmau, la Internet es un medio muy versátil para realizar diferentes actividades, por lo que gran índice de la población mundial la utiliza en diferentes partes territorios y al mismo tiempo logrando el flujo de información y comunicación.

Sin embargo, la red no es perfecta ni es completamente segura, nos encontramos con que en la Internet hay riesgos al momento de utilizarla, por ello ahora nos enfocaremos en hablar de las desventajas de ella y en precisar cómo es que la red es un medio para que se comisionen los ciberdelitos.

Para situarnos en el contexto acudimos a Suarez-Mira para precisar:

Cuando hablamos de ciberdelitos nos referimos a aquellas infracciones penales cuya ejecución tienen en Internet una de sus vías de comisión predilectas, si bien también son perfectamente realizables a través de otros caminos tal como acontecía antes del nacimiento de la red de redes[40].

Es decir, los ciberdelitos son todas aquellas conductas contrarias a la ley que utilizan a la Internet, como su instrumento o medio para comisionar el delito que afecta bienes jurídicos tutelados, sin importar si la víctima del delito es usuaria o no usuaria de la red.

Los ciberdelitos comprenden una gran gama de delitos, van desde aquellos que afectan en contra de la intimidad, el patrimonio, la paz y la seguridad de las personas; estos bienes jurídicos son agredidos con diferentes conductas, como por ejemplo el acceso ilícito a sistemas y equipos de informática; daño informático; intromisión informática; sabotaje informático; manipulación informática; piratería informática; *hacking;* pornografía infantil; ciberbullyng, usurpación de identidad; fraude informático; trata de personas; delincuencia organizada; entre otras más.

Las conductas anteriormente señaladas se basan completamente de la Internet para ser efectuadas, realizadas y consumadas. Así pues, desde sus inicios

[40] Suarez-Mira Rodríguez, Carlos, *op. cit.,* p. 117.

en la década de 1960 (véase la página 5) la Internet se ha convertido en pieza fundamental de la cibercriminalidad donde favorece la criminalidad de cuello blanco.

> Salom Clotet menciona que: la red no contempló en su origen la necesidad de establecer unos parámetros de seguridad necesarios para los servicios a los que luego se destinaria. Esto ha supuesto arrastrar desde su origen unos sistemas y protocolos que en sí mismos, presentan vulnerabilidades frente a las necesidades de confidencialidad, integridad y disponibilidad que hoy requieren[41].

Al respecto, estimamos que en la actualidad falta establecer en la legislación mexicana disposiciones aplicables para que los usuarios de la red usen de forma obligatoria mecanismos de seguridad informática, con el objeto de que estos mismos se protejan.

Por ende, si una computadora o sistema informático no cuenta con mecanismos de seguridad (como por ejemplo un antivirus) surgen vulnerabilidades a estos mismos, lo que conlleva a que personas con demasiada pericia en el campo de los sistemas informáticos y en redes utilicen sus conocimientos para comisionar el ciberdelito.

De esta manera, el cibercrimen no tiene fronteras, porque Internet tampoco las tiene, la gran red de redes permite que desde una locación remota y escudado bajo el "anonimato" que le brinda estar detrás de un teclado, un individuo pueda cometer un delito en otra jurisdicción, en otro país o en otro continente[42].

Lo anterior es otra desventaja, pauta o traba que se presenta en la lucha contra esta nueva forma de criminalidad, pues la Internet al ser una red trasnacional de carácter mundial, ofrece la expansión del ciberdelito hacia todo el mundo en donde se tenga el acceso a la red.

---

[41] Salom Clotet, Juan, "Delito informático y su investigación", *Delitos en contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, España Consejo General del Poder Judicial, 2006, p. 97

[42] Salis, Ezequiel, "Desafíos de la investigación de los delitos informáticos en la "Deep & dar web"", en Dupuy Daniela (Dir.), *Cibercrimen*, Argentina, Euros editores, 2016, p. 601.

Por lo tanto, una persona puede comisionar el ciberdelito utilizando la Internet como un instrumento a su favor; asimismo, las distancias no son un obstáculo pues el ciberdelito se puede realizar desde un país que se encuentre cerca o a miles de kilómetros de distancia donde esté la víctima.

> Con la expansión global de la red en el nuevo milenio, formas de delito tradicionales adoptaron nuevas modalidades mediante el uso de las tecnologías emergentes. Tras el surgimiento de sitios comerciales en línea, delitos económicos como el fraude, la estafa y las falsificaciones expandieron sus fronteras por el uso de este nuevo intercambio[43].

A causa de la inmensidad de la red y a la vez de su vulnerabilidad se han presentado nuevos casos de delitos, donde los delitos tradicionales han evolucionado, o bien, han tomado nuevas formas de comisionarse, como por ejemplo, el delito de fraude en determinados supuestos se ha convertido en fraude informático, el daño a daño informático y el delito de amenazas adquiere la modalidad de realizarse por medio de la Internet conformándose el denominado Ciberbullyng o ciberacoso.

De esta manera, vemos que la web ofrece grandes facilidades para la comisión de los ciberdelitos, estas facilidades conllevan a que el público en general puedan ser la víctima o el victimario como usuarios de la red, los cuales actualmente son bastantes en todo el mundo.

> Asimismo, Almenar Pineda expresa que en los años noventa, la llegada de Internet para el público en general supuso el acceso el intercambio de una cantidad ingente de información, prácticamente en cualquier parte del mundo. Los datos prohibidos en un país llegaban vía Internet desde otro país. El hacking no es una excepción al incremento de estos delitos[44].

[43] Sain, Gustavo Raúl, *Delito y nuevas tecnologías,* Argentina, Editores del Puerto, 2012, p. 7.
[44] Almenar Pineda, Francisco, *El delito de hacking,* España, Editorial Arizandi, 2018, pp. 45 y 46.

Efectivamente, en esta década comienza el auge de la Internet (véase las páginas 9 y 10), esto se debió a la creación de la WWW con la que la mayoría de las personas, empresas y el Gobierno, se querían conectar a la red y ser suma del ciberespacio, lo que actualmente nos ofrece acceder a millones de páginas web de todo el mundo.

Sin embargo, ante todos los beneficios que ofrece la Internet las conductas ilícitas no se hicieron esperar, por lo que consecutivamente a ello fue que especialistas y curiosos en los sistemas informáticos se dedicaron a comisionar ciberdelitos en gran aumento y el cibercrimen se ha convertido en un fenómeno mundial.

> Así pues, Internet supone la elevación de los delitos informáticos del ámbito local o regional a un nuevo ámbito global, razón por la cual la ONU dicta la resolución 45/121 de 14 de diciembre de 1990 donde son atendidas las nuevas formas de criminalidad y en 1994 emitió el Manual para la prevención y el control de los delitos relacionados con la informática[45].

Por ende, debido al aumento de este fenómeno de conductas antijurídicas de característica global, la ONU busca soluciones con la finalidad de dar respuesta a esta problemática, por lo que dicta el Manual anteriormente citado para que los Estados Miembros retomen sus recomendaciones y procuren la prevención del ciberdelito.

## II. INFORMÁTICA

La informática se ha convertido un factor muy importante en el desarrollo de México, ésta, ha traído consigo cambios evolutivos en los aspectos económicos, culturales, sociales, políticos, educativos, tecnológicos y científicos, de los cuales, los mexicanos, nos hemos beneficiado de forma constante.

[45] Idem, 46.

Con esta herramienta no sólo se han creado nuevas investigaciones, también ha sido de gran utilidad para el campo del derecho a través de la informática jurídica en el actuar del sector público y privado por su funcionamiento de guardar, compartir y difundir información de forma automatizada.

De esta manera, la informática resulta ser un instrumento muy importante para el mejor conocimiento y aplicación de derecho, sobre todo si se la vincula con sus temas básicos, como la simplificación del orden jurídico, el acceso de la población al derecho y la actualización de los juristas[46].

Sin duda, con el apoyo de la informática se han proporcionado muchos beneficios, pero, con su proliferación mayúscula de los sistemas informáticos surge la facilidad para que nazcan nuevos tipos delictivos, tipificados como delito de Acceso ilícito a sistemas y equipos de informática, delitos informáticos, y conceptualizados por la ciencia jurídica como ciberdelitos, delincuencia informática, y entre otras denominaciones que autores les han dado.

Un delito informático es una conducta típica, antijurídica y culpable, cometida por una persona especialista en el campo de la informática, es decir, los expertos en el manejo de sistemas informáticos, se han aprovechado de la vulnerabilidad informática y de las habilidades que ellos mismos poseen para cometer este tipo actos ilegales.

Por ende, si un equipo informático no se protege de la forma y con las medidas y mecanismos de seguridad adecuados, está inmerso a ser receptor de un ataque a su sistema, causando en él, un daño grave que puede ser total o parcial según cual sea el objetivo del mismo.

Un ataque informático implica desde usar, entrar, interceptar o interferir, agredir la base de datos de una computadora, red o sistema informático, sin la

[46] Hernández Camargo, Emiliano, *La informática jurídica y legislativa en México,* México, Consejo Nacional de Ciencia y Tecnología, p. 12.

autorización previa del dueño, con el ánimo y propósito de provocar pérdida y/o apoderamiento de información, alterando o dañando el sistema.

Asimismo, con el desarrollo que presenta la informática hoy en día, y como ya referimos en párrafos anteriores, es una fuente productora de ciberdelitos, por lo que se le debe de dar una especial atención en su tratamiento jurídico para evitar que se comisione esta conducta delictiva; por consiguiente, ahora describiremos la conceptualización de informática.

1. *Concepto de informática*

Existen un sin fin de conceptos de informática, entre los cuales destaca Hernández Camargo quien nos dice:

> En la perspectiva etimológica se entiende como resultado de la fusión de los términos información y automatización. Esta es la posición asumida por Phillipe Dreyfus a partir del año de 1962. Fue establecido en Francia, se unieron las dos primeras silabas de *information*, "información", y las tres últimas de *automatique*, "automática", por lo que el neologismo, da a entender claramente la intención al referirse a "información automatizada", más explícito, al "tratamiento automático de los datos que constituyen la información"[47].

Del concepto etimológico trazado por Hernández Camargo, inferimos que el objeto principal de la informática es atender el procesamiento automático de la información y de los datos electrónicos almacenándolos en el propio sistema informático para su uso.

Por otra parte, para Sánchez Montufar la informática es el estudio del tratamiento automático de la información. La informática nace debido a la necesidad

[47] *Ibídem,* p. 5.

de analizar, de algún modo, los datos y procesarlos para obtener información, la cual se pueda almacenar y recuperar posteriormente de manera automática[48].

Ante lo claro y concisos que fueron los conceptos anteriores, elaboramos nuestra propia concepción y referimos que la informática es el conjunto de sistemas informáticos sistematizados, que tiene como objetivo regular el tratamiento automático de la información almacenada en ellos.

Entendido el concepto de informática daremos continuidad a describir los antecedentes relacionados con su origen, su construcción, desarrollo y perfeccionamiento; explicando cómo se proliferó globalmente logrando la consideración de ser una de las herramientas profesionales más importantes debido a las utilidades que nos ofrece.

2. *Antecedentes de la informática*

El inicio de la informática, denota con la invención de la maquina analítica creada por el científico matemático Charles Babbage en 1834, después de esto, diferentes científicos (cada uno en diferentes años) innovan la máquina analítica de Babbage, aportándole diferentes funcionamientos, para convertirla en lo que hoy conocemos como computadora, PC, o Laptop.

Charles Babbage es considerado como el padre de la informática, por su gran apego a la creación e innovación de la máquina analítica pues trabajó en ella hasta su muerte, y por otro lado, Alan Turing se le atribuye ser padre de la informática moderna porque sus grandes ideas fueron la base para que se avanzara en el desarrollo tecnológico de los ordenadores electrónicos.

Aclarando, antes de la máquina analítica de Charles Babbage, ya se habían inventado otras máquinas como la *pascaline,* y la aportación de Gottfried Wilhelm Von Leibniz, no obstante, estas máquinas no forman parte de la informática

[48] Sánchez Montúfar, Luis, *Informática,* México, Pearson Educación, 2005, p. 18.

moderna pues estas no eran analíticas, pero su invención fue de gran ayuda, para que Babbage pudiera crear su máquina, por eso señalaremos su creación.

Villarreal de Anaya afirma que fue de esta manera que, a mediados del siglo XVII (1642), el filósofo, matemático y teólogo francés, Blas Pascal, inventó la primera calculadora mecánica que tenía una serie de engranajes o ruedas dentadas que le permitía realizar sumas y restas[49].

Ante la necesidad de hacer altas operaciones numéricas, matemáticos empezaron este proyecto de inventar una maquina (actualmente calculadora), que pudiera contar, y a la vez, que lo hiciera de forma automatizada, desde esta época, se fue elaborando este proyecto de construcción e innovación de las computadoras.

De esta forma, Sánchez Montufar nos dice que en la década de 1820 Charles Babbage comenzó a desarrollar su máquina diferencial, un aparato que podía realizar cálculos matemáticos sencillos. Este dispositivo mecánico fue creado para calcular tablas de números que eran útiles para la navegación[50].

En consecuencia, observamos que el antecedente de origen de la informática fue la invención de la calculadora, pues los matemáticos querían efectuar grandes cálculos de manera automática, pero, aún no se imaginaban que la tecnología fuera a evolucionar tanto al punto de crear la computadora.

Asimismo, la máquina diferencial de Babbage se convirtió en un proyecto de gran utilidad para las instituciones Gubernamentales Británicas y banqueros, pues estos la utilizaban para hacer grandes cálculos y les facilitaba las tareas que realizaban gracias a su función.

Posteriormente, en 1834, Babbage, concibió la idea de una maquina analítica, que era una computadora de propósitos generales. Conforme a su diseño,

[49] Villareal de Anaya, Sonia, *Introducción a la computación: guía práctica para el aprendizaje de paquetes,* México, McGraw-Hill Interamericana Editores, 1999, p. 25.
[50] Sánchez Montúfar, Luis, *Informática, op. cit.,* p. 3.

la maquina podía sumar, restar, multiplicar y dividir a una velocidad de sesenta sumas por minuto[51].

Después de catorce años, Babbage modifica su máquina diferencial evolucionándola a máquina analítica volviéndola más rápida, ésta fue una pieza clave para seguir con el proceso del proyecto de creación de las computadoras electrónicas. Después de Babbage por varias décadas hubo ausencia en la realización del proyecto de formación de las computadoras.

> Como menciona Garriga Domínguez, en 1936 Alan Turing realizaba el diseño abstracto de ordenador estableciendo los principios que supusieron el mayor avance teórico que condujo al nacimiento de la informática. Sus descubrimientos aportaron enormes progresos tanto en fundamentos lógicos como en el desarrollo de la computación[52].

Como ya se mencionó Alan Turing es considerado el padre de la informática moderna, siendo valorado como un gran científico de la computación, con su invento denominado como la primera computadora electrónica marca un nuevo camino hacia el proceso evolutivo de las computadoras electrónicas automáticas, lo que amplía el camino para que demás técnicos en informática inventen más computadoras innovando cada vez más la ya existente.

En 1945 el matemático John Von Neumann, llevó a cabo un estudio teórico que demostraba que la computadora, podía tener una estructura física muy sencilla y capaz de ejecutar eficientemente cualquier tipo de cálculo a través de control programado, sus ideas son referidas como la técnica del programa almacenado[53].

John Von Neumann marca tendencia con su ingenio de agregarle a la computadora un sistema de almacenamiento interno, para que los datos permanecieran en el interior de la computadora y no en las tarjetas perforadas que

---

[51] *Ibídem,* p.5
[52] Garriga Domínguez, Ana, "El impacto de las TIC en los derechos humanos, en Garriga Domínguez, Ana (coord.) Fundamentos éticos y jurídicos de las TIC, España, Editorial Aranzadi, 2012, p. 69.
[53] Villareal de Anaya, Sonia, *op. cit.,* p. 28.

se utilizaban en las décadas anteriores, esto sin duda fue de gran importancia para el avance en las próximas computadoras electrónicas.

Después de este periodo se clasifican a las computadoras por seis generaciones:

En los años de 1951 a 1959 se considera la primera generación de computadoras. Se caracterizaban por ser maquinas muy grandes y costosas, que tenían una ínfima potencia en comparación con los actuales ordenadores personales[54].

Sin duda, la primera generación de computadoras no fueron nada parecidas a las que tenemos actualmente, estas eran muy grandes, posteriormente se convirtieron en más pequeñas, con mayor almacenamiento de información y más veloces.

La segunda generación comprendida entre 1955 a 1968, las computadoras estaban constituidas por transistores, se programan en nuevos mensajes llamados "lenguajes de alto nivel", eran de tamaño más reducido, su costo es menor, más compañías las fabricaban y los equipos eran bastante avanzados para la época[55].

En esta segunda generación, el costo de las computadoras disminuye ante la producción y la demanda, pues más compañías las empiezan a fabricar, y a comercializar, sin embargo, estas aún eran costosas, y por lo tanto sólo las seguían adquiriendo compañías de capital alto.

> Por otra parte, Ferreyra Cortes manifiesta que otro gran logro de esa época es el desarrollo del primer lenguaje de alto nivel, el FROTAN (*FORmula TRANslator*). John Backus y alguno de sus colaboradores empleados del IBM *(International Business Machines Corporation)*, empezaron este proyecto en 1954 y lo presentaron formalmente en 1957[56].

---

[54] Garriga Domínguez, Ana, *op., cit.,* p. 70.
[55] Sánchez Montúfar, Luis, *Informática, op. cit.,* p. 11.
[56] Ferreyra Cortés, Gonzalo, *Informática para cursos de bachillerato,* México, Alfaomega Grupo Editor, 2000, p. 32.

Estos científicos perfeccionaron el lenguaje antiguo de las computadoras en uno más avanzado convirtiéndola en más veloz, útil para que las computadoras fueran más comerciales.

> En 1960 las computadoras seguían evolucionando reduciendo su tamaño y aumentando su capacidad de procesamiento. Posteriormente aparece la PC *(Personal Computer),* con mejores circuitos, más memoria, unidades de disco flexible. Aparecen los programas procesadores de palabras como el *Word Star,* y la hoja de cálculo creada por Dan Bricklin y Bob Frankston en 1979. Las empresas comenzaron a utilizar las computadoras para tareas de almacenamiento de registros, manejo de inventarios, nómina y contabilidad[57].

Con el invento de la PC, un usuario ya podía acceder a hojas de texto para escribir, o bien acceder a hojas de cálculo para automatizar datos matemáticos, y a la vez, en ella ya se podía almacenar información, lo cual era algo nuevo en estas fechas marcando gran impacto, sin embargo, sólo se podía utilizar por una persona a la vez, es por ello su denominación, *Personal Computer.*

A mediados de la década de 1960 ocurrió la mayor transición en tecnología de las computadoras. Las computadoras de transistores fueron sustituidas por maquinas más pequeñas y poderosas, construidas con circuitos integrados. Estos contenían miles de pequeños transistores en chips de silicio, ahorrando espacio[58].

Durante la década de 1960, con la creación de esta nueva tecnología de computadoras, se permitió el nacimiento de la tercera generación de computadoras (1965-1970), convirtiéndolas en más pequeñas y con velocidad haciéndolas más productivas.

Posteriormente, en 1971 *Intel Corporation,* que era una pequeña compañía fabricante de semiconductores ubicada en Silicon Valley, presenta el primer

---

[57] Sánchez Montúfar, Luis, *Informática, op. cit.,* p. 12.
[58] Villareal de Anaya, Sonia, *Introducción a la computación: guía práctica para el aprendizaje de paquetes. op. cit.,* p. 28.

microprocesador o chip de 4 bits, que en un espacio de aproximadamente 4x5 mm contenía 2,250 transistores[59].

Con la aparición de chips de memoria o microprocesadores se inicia la cuarta generación de computadoras comprendida de 1971 a 1984. Algunos autores consideran que la cuarta generación de computadoras fue la última, otros consideran que con la tercera generación se termina debido a los cambios tecnológicos que se han dado en las últimas décadas, otros consideran que existe una quinta y sexta generación, por lo cual, es oportuno para esta investigación aludirlas.

> Con base a los grandes acontecimientos tecnológicos en materia de microelectrónica y computación, a mediados de la década de los años ochenta se establecieron las bases para lo que se puede considerar como quinta generación de computadoras (1984 a 1990). Las computadoras de esta generación contienen una gran cantidad de microprocesadores trabajando con la capacidad de comunicarse con un lenguaje natural e irán adquiriendo la habilidad de tomar decisiones (sistemas expertos e inteligencia artificial)[60].

Las computadoras de esta generación ya se encontraban vinculabas directamente con la Internet, pues la red se había a proliferado como un sistema grande de redes interconectadas en diferentes países del mundo, por lo tanto, las computadoras se empezaron a incorporar masivamente en empresas de gran prestigio, instituciones científicas y en universidades para ser utilizadas como medio de comunicación y como almacenamiento de datos.

La sexta generación de computadoras denota de 1990 a la actualidad, estas computadoras cuentan con arquitecturas combinadas Paralelo/Vectorial, con cientos de microprocesadores vectoriales trabajando al mismo tiempo, capaces de realizar más de un millón de millones de operaciones por segundo[61].

---

[59] Ferreyra Cortés, Gonzalo, *Informática para cursos de bachillerato, op. cit.,* p. 35.
[60] *Ibídem,* p. 39.
[61] *Ibídem.,* p. 40.

Esta sexta generación en la cual estamos inmersos hoy en día, las computadoras cuentan con una inmensa tecnología tanto las de escritorio como las portátiles (Laptops), tablets, su diseño físico y su capacidad de almacenamiento de información y de rapidez es impresionante.

Sin duda, el avance del desarrollo de las computadoras sigue y seguirá creciendo día con día, haciéndolas cada vez más potentes, y con un lenguaje más inteligente, por lo que en las próximas décadas por venir, tal vez se cierre esta sexta generación y se establezca una séptima y subsecuentes generaciones de computadoras con tecnología más novedosa que la que actualmente tenemos.

Al próximo desarrollo que se efectuará en las décadas supervinientes, faltará que los ingenieros informáticos se preocupen, y asimismo se ocupen en hacerlas menos vulnerables para que no se utilicen como medio, instrumentos u objeto material de delitos.

3. *La informática como el medio y el objeto del delito de Acceso ilícito a sistemas y equipos de informática*

La informática hoy en nuestros días es una herramienta utilizada con bastante frecuencia para facilitarnos las distintas tareas que realizamos, en ese sentido, las computadoras se han globalizado por gran parte del mundo pues son la pieza clave para procesar y almacenar información.

De la misma manera que la informática permite la expansión del conocimiento, la información, la cultura etcétera, también abre las puertas a la proliferación de numerosas actividades inapropiadas, pudiendo facilitar la comisión abusos a derechos fundamentales y afectar bienes jurídicos[62].

Como manifiesta Suarez-Mira la informática aparte de ser un instrumento que posee grandes beneficios tanto a la sociedad como en el uso personal, también se

[62] Suarez-Mira Rodríguez, Carlos, *op., cit.,* p. 103.

ha convertido en el instrumento principal para que se comisionen actos contrarios a la ley.

En ese sentido, la conducta antijurídica atenta contra los bienes jurídicos tutelados por el legislador, como los son los bienes de la intimidad y protección a los sistemas informáticos cuando se afecta a la información contenida en los sistemas y equipos informáticos, sea esa información de índole personal, gubernamental, empresarial, o de cualquier otra.

Así pues, Gustavo Sain sostiene que: ya con el inicio de las comunicaciones mediadas por las computadoras durante los años 60, diferentes tipos de conductas indebidas o licitas comenzaron a aparecer entre los usuarios conectados a los centros académicos y laboratorios de investigación de aquel entonces[63].

Desde la proliferación de la informática, los ataques a los sistemas informáticos no se hicieron esperar, así es como aparecen diferentes conductas como las son el acceso ilícito a los sistemas informáticos, lo que conlleva a conformarse una nueva forma de criminalidad, conocida actualmente como cibercriminalidad.

> De la misma, manera Sáez Capel refiere que: este tipo de conductas surgen desde el momento en que el uso de los sistemas informáticos abre nuevas formas de ataque a los bienes jurídicos protegidos y aparecen nuevas situaciones de desconocidas antes de entonces, de ahí que se trate de conocer las nuevas conductas merecedoras de la sanción penal[64].

Asimismo, la cibercriminalidad a los sistemas informáticos aparece como nueva conducta ilícita con las modalidades de *hacking*, sabotaje informático, intromisión informática entre otras más con el objetivo de modificar, destruir o provocar perdida de información electrónica.

---

[63] Sain, Gustavo Raúl, *op. cit.,* p. 2
[64] Sáez Capel, José, *Informática y delito,* 2a. ed., Argentina, Proa XXI editores, 2001, pp. 41 y 42.

En el uso de las nuevas tecnologías actualmente concurren una serie de factores como lo es un precipitado acceso a ellas, lo que facilita la causación de daños imprudentes en los sistemas informáticos y la obstaculización en su normal funcionamiento e incluso el acceso ilícito a ellos[65].

En consecuencia, el incremento de la informática, así como también su vulneración, ha provocado que esta nueva forma de criminalidad tenga tantas modalidades con las que puede ser cometido el ciberdelito (las que describiremos en el siguiente capítulo) y cada una de ellas deben de estar contempladas en la ley.

Se habla de criminalidad informática como de una categoría criminal, tal como apunta Tiedemann, se trata de proteger no tanto bienes jurídicos distintos de los ya protegidos, siendo la tarea fundamental determinar las conductas, que sean realmente nuevas y que justifique hablar de delincuencia informática[66].

Análogamente, a lo referido por Saéz Capel, inferimos que el delito Acceso ilícito a sistemas y equipos de informática es una criminalidad informática de nueva tendencia, es decir, antes de la creación de la informática así como también de su expansión, jamás se hubiera imaginado que podría existir este tipo de delito.

Por ende, al surgir este tipo de delito es que también se originan nuevos bienes jurídicos a tutelar lo que conlleva a tipificar estos nuevos tipos penales de forma urgente con el objeto de frenar los actos ilícitos que se desprenden de la cibercriminalidad.

En los últimos años la mayoría de los ordenamientos jurídicos han consagrado el denominado “derecho a la libertad informática”, como un nuevo derecho que permite a los sujetos sustraer del conocimiento ajeno determinadas esferas de su vida, impidiendo así el tratamiento indiscriminado y sin control de determinadas informaciones y datos personales[67].

---

[65] Almenar Pineda, Francisco, *op., cit.* p. 31.
[66] Sáez Capel, *op. cit.,* p. 42
[67] Menéndez Mato, Juan Carlos y Gayo Santa Cecilia, Ma. Eugenia, Derecho e informática. Ética y legislación, España, Bosch Editor, 2014, p.271.

Así pues, en México en el año de 1999 nace el derecho a la libertad informática, el cual es tutelado por el Código Penal Federal y por los diferentes Códigos penales estatales, para prevenir y sancionar las conductas típicas, antijurídicas y culpables que lesionan al contenido de los sistemas informáticos.

> Asimismo, Aboso plantea: en la moderna sociedad de la información y las comunicaciones, las agresiones cometidas contra la integridad de los sistemas, programas y datos informáticos representan un nuevo desafío para el Derecho Penal. El uso de programas dañinos, la interceptación de comunicaciones telemáticas, la alteración de datos personales, entre otras manifestaciones lesivas tienen por objeto a integridad funcional de los sistemas informáticos[68].

Ante esas agresiones a la información contenida en la informática, es que se tipifica por el Código Penal Federal el delito de acceso ilícito a sistemas y equipos de informática, incorporando al capítulo de revelación de secretos en los artículos 211 bis 1 al 211 bis 7.

De lo previo, nos surgen las siguientes cuestiones ¿este delito se tipifica en forma correcta?; ¿Todas las diversas modalidades antijurídicas de la informática son encuentran contempladas por el Código Penal Federal?; ¿Existe una uniformidad, homologación y armonía legislativa en México para este tipo de delito por el Código Penal Federal y los Códigos Penales de las entidades federativas?; en el siguiente capítulo analizaremos dichos planteamientos.

[68] Aboso, Gustavo Eduardo, *Derecho penal cibernético,* Argentina, euros editores, 2017, p. 1.

# CAPÍTULO SEGUNDO

## CONDUCTAS DELICTIVAS QUE AFECTAN EL SECRETO INFORMÁTICO Y SU TIPIFICACIÓN EN MÉXICO

Reiteramos, la tecnología informática es una de las herramientas más indispensables en el incremento del flujo de la información y la comunicación en la sociedad actual, las que se utiliza en la vida diaria para realizar diferentes actividades. Esta herramienta que forma parte las Tecnologías de la Información y de la comunicación es conocida como TIC´S, nos abren las puertas en el entorno internacional logrando acrecentar actividades que van más allá de las comerciales, científicas y sociales.

Por ello, Villa Escobosa afirma que la informática, las tecnologías y las herramientas asociadas a ésta, no están exentas de que los delincuentes busquen la manera de utilizarlas para lastimar a las personas en su integridad física o moral, en su patrimonio, en su salud, en su seguridad, etc.[69].

Así pues, desde el desarrollo de la informática las personas comenzaron a interesarse por usar los medios electrónicos, y de igual manera, otras personas con habilidades en la misma área, se interesaron en obtener provecho de la informática para sí mismos, causando daño a la información contenida, o a utilizándola como medio para afectar bienes jurídicos.

Estas conductas se han tipificado en el Código Penal Federal y por los diversos Códigos Penales de los estados mexicanos, como Acceso ilícito a sistemas y equipos de informática (entre otras denominaciones más), para así sancionar, y evitar el cibercrimen en los ámbitos de orden federal y del fuero común.

La Internet no conoce barreras territoriales, es de carácter universal, por lo tanto estas conductas forman a ser interestatales, impregnándose en todos los

[69] Villa, Escobosa, Jaime, "Los delitos informáticos", en Durán Díaz, Oscar Jorge (coord.), *Derecho y medios electrónicos, temas selectos,* México, Porrúa, 2012, p. 227.

estados del territorio mexicano, causando graves estragos que afectan los bienes jurídicos de las personas, y por subsecuente también a la sociedad.

En esta tesitura, es cuando se recurre al Derecho Penal, como instrumento regulador de prevención y sancionador de conductas delictivas, con el objetivo de que mantenga activo el orden social dentro de un territorio, garantizando la tutela de bienes jurídicos fundamentales.

Conforme a lo anterior, y para mayor precisión del contenido, daremos a señalar unos conceptos previos al tema:

## I. CONCEPTOS PREVIOS

### 1. *Sistema informático*

Paloma Parra cita al Convenio sobre Cibercriminalidad de Budapest del 23 de noviembre de 2001, quien define el concepto de sistema informático como: el sistema informático designa todo tipo de dispositivo aislado o conjunto de dispositivos unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos[70].

En otras palabras, el sistema informático, es un sistema de cómputo que se compone por un conjunto de un *hardware* y de un *software,* diseñados con programas informáticos especializados que permiten almacenar y procesar datos informáticos dentro de él mismo.

### 2. *Datos informáticos*

Los datos informáticos designan toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático, ejecute una función[71].

[70] Paloma Parra, Luis Orlando, *Delitos informáticos (en el ciberespacio),* Colombia, Ediciones jurídicas Andrés Morales, 2012, p. 22.
[71] *Idem.*

Es decir, los datos informáticos son todo el conjunto de información en forma de códigos, contenida y almacenada en el sistema o equipo informático, que requiere de un tratamiento informatizado por parte del mismo, para su almacenamiento y procesamiento.

3. *Archivos de documentos electrónicos*

> Esteban Navarro especifica que son, el conjunto de documentos producidos, recibidos o reunidos por una persona física o jurídica, haciendo uso de la electrónica, que se conservan y se transmiten mediantes medios electrónicos, con el fin de garantizar su valor informativo legal y cultural así como permitir su acceso y uso también mediante las tecnologías de la información y la comunicación[72].

Por ende, los archivos de documentos electrónicos, son aquellos producidos por el actuar del hombre mediante los diferentes dispositivos electrónicos, para darles un tratamiento automático e informatizado a sus información con el propósito de que satisfagan ciertas necesidades.

4. *Base de datos*

> Peña Tresancos nos dice, una base de datos es un programa, que permite almacenar datos de forma organizada y obtener información acerca de esos datos. Existen distintos tipos de bases de datos. En las más simples, la base de datos es el archivo que almacena datos y nos permitirá ordenarlos o extraer los que cumplen una determinada condición simplemente describiendo la orden adecuada[73].

Dicho de otro modo, una base de datos es cualquier archivo electrónico que contiene datos informáticos; en otras palabras, una base de datos es un archivo que

---

[72] Esteban Navarro, Miguel Ángel, *"Los archivos de documentos electrónicos",* El profesional de la información, España, Vol. 10, Número 12, Diciembre de 2001.
[73] Peña Tresancos, Jaime y Vidal Fernández, María Carmen, *Introducción a la informática*, España, McGraw-Hill/Interamericana de España, 2004, p. 6.

almacena información de diversa índole, sea personal, comercial, gubernamental o financiera.

5. *Hardware*

Por su parte, Norton Peter menciona que, los dispositivos mecánicos que conforman la computadora se llaman *hardware.* El *hardware* es cualquier parte de la computadora que se puede tocar; consiste en dispositivos electrónicos interconectados que puede utilizarse para controlar una operación[74].

Al ser el *hardware* cualquier parte de la computadora que se puede tocar, constituye a ser la parte física de la computadora, lo que se conforma por el monitor, teclado, CPU, mouse (ratón), cables, impresoras, bocinas, memorias de almacenamiento, CD o Diskets.

6. *Software*

Los programas que permiten que funcione el ordenador son el *software.* Contienen las instrucciones que determinan el funcionamiento de todos sus elementos electrónicos, para que hagan las operaciones que deseamos con los datos que le vamos a introducir[75].

Por el contrario al *hardware,* el *software* es la parte interna de las computadoras o dispositivos electrónicos, es decir, no podemos apreciar su físico, se conforma de un conjunto de programas operativos que van encaminados a hacer que las computadoras realicen sus tareas.

7. *Programa*

Son aquellos que utilizan los usuarios para realizar sus trabajos; son los programas de procesador de textos, las hojas de cálculo, las bases de datos, los programas de dibujo y tratamiento de imágenes, etc. Algunos de estos programas se emplean para realizar tareas muy concretas[76].

---

[74] Norton, Peter, *Introducción a la computación,* 6a. ed., México, McGraw-Hill/Interamericana Editores, 2006, p. 25.
[75] Peña Tresancos, Jaime y Vidal Fernández, María Carmen, *op. cit.*, p. 6.
[76] *Idem.*

Como ya referimos, el programa es un fragmento del sistema operativo *software*, existen demasiados tipos de programas para los ordenadores, cada uno de ellos tiene por objeto ejecutar una serie de tareas específicas mediante instrucciones concretas. Los programas más básicos para el funcionamiento de la computadora ya vienen previamente instalados, y los que desarrollan tareas más peculiares necesitan ser comprados o descargados en la web, por ejemplo, Microsoft Office, Adobe, Antivirus, Photoshop, CorelDRAW, entre otros, conforme a las necesidades que el usuario tenga.

8. *Acceso a un sistema informático*

> Por otra parte, acceso significa, introducirse o ingresar a un sitio determinado; por ello, se requiere siempre de autorización de quien tiene ese control de ingreso a un lugar en específico, y para acceder a un sistema informático se debe tener en cuenta que, "el control de acceso implica, quien tiene el acceso a sistemas informáticos específicos y recursos en un momento dado"[77].

Es decir, un acceso a un sistema informático requiere de una autorización previa por el dueño del equipo o sistema informático, sino se establece esa autorización, y se decide acceder al equipo o sistema informático, esa conducta de acceso será de forma ilegal, por lo que a la vez se comete un delito.

De esta manera, Téllez Valdez refiere que el acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo con uno de los diferentes medios existentes. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad o en los procedimientos del sistema[78].

Los accesos a los sistemas informáticos se pueden cometer sin que el sujeto activo se encuentre físicamente en el equipo donde quiere acceder, esto se puede llevar a cabo con la ayuda de la Internet, debido a que la red tiene su expansión en la mayor parte del país.

---

[77] Paloma Parra, Luis Orlando, *op. cit.*, p. 32

[78] Téllez Valdés, Julio, *Derecho informático,* 4a ed., México, McGraw Hill Interamericana, 2009, p. 195.

9. *Seguridad informática*

> Es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos y bloquear el acceso de usuarios autorizados al sistema[79].

En este sentido, la seguridad informática es un mecanismo de protección para el equipo, sistema o red informática, el cual, su función consiste en impedir que se cometan accesos ilícitos a los equipos resguardando toda la información contenida en estos mismos.

Aunado a lo anteriormente señalado, procederemos a describir primeramente el concepto de delito, debido a que es pertinente para esta investigación señalarlo, para precisar el fenómeno antisocial relacionado con el delito de Acceso ilícito a sistemas y equipos informáticos.

## II. CONCEPTO DE DELITO

A lo largo del tiempo, el concepto de delito ha ido definiéndose por diferentes tratadistas del Derecho Penal, cada uno de ellos ha agregado nuevos elementos a la conceptualización de este mismo, conformándolo a como hoy lo estudiamos, por lo que aquí señalaremos los más relevantes.

Para el autor Francesco Antolisei en su obra titulada Manual de Derecho Penal, menciona sistemáticamente que el delito, en general, se define como todo hecho por el cual el ordenamiento jurídico le adscribe como consecuencia una pena[80].

Por lo tanto, para este autor el delito incorpora una sanción a toda persona que por acción u omisión quebrante el ordenamiento jurídico que rige vigentemente,

---

[79] Gómez Veitetes, Álvaro, *Enciclopedia de la seguridad informática*, México, Alfaomega grupo editor, 2007, p. 3.

[80] Antolisei, Francesco, *Manual de derecho penal,* 8a. ed., trad. Jorge Guerrero y Marino Ayerra Redín, Colombia, 1988, P. 115.

el cual, conlleva en sí mismo una penalidad interpuesta por la disposición de la norma jurídico penal.

Para Ernesto Beling citado por Luis Jiménez de Asúa en la obra Lecciones del Derecho Penal, menciona que el delito es la acción típica antijurídica culpable, sometida a una adecuada sanción penal que conlleva las condiciones objetivas de penalidad[81].

En esta concepción Ernesto Beling incorpora la figura de la tipicidad al concepto de delito que ya venían trabajando autores anteriores, al precisar que toda conducta ilícita debe de estar plasmada como delito en el texto de la ley previamente al caso, con el cual también se atiende al principio de legalidad.

En suma, el delito también es definido en el libro primero del Código Penal Federal vigente (fecha de última reforma 12 de abril de 2019), por el artículo séptimo el cual, lo precisa como: el delito es el acto u omisión que sancionan las leyes penales.

En esta concepción de delito, se contempla su carácter sancionador, para toda persona que infrinja la ley, ya sea por acción u omisión a la conducta previamente tipificada como delito por las normas jurídico penales vigentes, con una pena y/o una medida de seguridad.

En los diferentes conceptos de delitos anteriormente señalados, vienen enmarcados variados elementos que son categorizados como positivos y negativos; en los elementos positivos podemos encontrar a la conducta (acción u omisión) tipicidad, antijuridicidad y culpabilidad.

Por otra parte, los aspectos negativos del delito son interpretados a *contrario sensu,* es decir, estos se refieren a la ausencia de conducta, atipicidad, causas de justificación e inculpabilidad que son los supuestos excluyentes del delito y por lo general no punibles contemplados en el artículo 15 del Código Penal Federal.

[81] Jiménez de Asúa, Luis, Lecciones de derecho penal, México, Oxford University Press, 1999, v III, p. 132.

Atendiendo a los elementos positivos del delito precisaremos sus definiciones, y estas mismas las ejemplificaremos con el delito de acceso ilícito a sistemas de cómputo y equipos de informática:

Pavón Vasconcelos define a la conducta, como el comportamiento del hombre que se traduce exteriormente en una actividad o inactividad voluntaria. Este concepto es comprensivo de las formas en las cuales la conducta pueda expresarse: acción u omisión[82].

La conducta por acción en el delito Acceso ilícito a sistemas y equipos de informática se traduce, cuando el sujeto activo se ocupa en acceder, sin o con autorización a un equipo o sistema informático para modificar, destruir, provocar perdida de información, interceptarlo, causando en él un daño total o parcial. La conducta por omisión no encuadra en este delito debido a que el sujeto activo no la puede cometer imprudencialmente, éste tiene el dolo de ingresar al sistema informático para ocasionar el daño a la información.

Raúl carranca y Trujillo nos dice que la tipicidad es la adecuación de la conducta concreta al tipo legal concreto; y para definir al tipo legal cita a Jiménez de Asúa, quien dice que tipo legal es, la abstracción concreta que ha trazado el legislador, que se cataloga en la ley como delito[83].

Conforme a lo anterior, podemos analizar que en las conductas ilícitas informáticas el tipo penal es lo descrito por los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal, mientras que la tipicidad es la conducta informática delictiva prohibida por estos ordenamientos jurídicos penales.

Atendiendo a la antijuridicidad, el autor Max Ernest Mayer define la palabra antijurídica en dos puntos de vista, como en una definición nominal y definición real: Antijurídica es una conducta humana que no está en concordancia con una norma jurídica, es decir, con un mandamiento o

[82] Pavón Vasconcelos, Francisco, *Manual de* D*erecho penal mexicano parte general,* 16a ed., México, Porrúa, 2002, p. 212.
[83] Carranca y Trujillo, Raúl, *Derecho penal mexicano parte general,* 15a ed., México, Porrúa, 1986, p. 423.

prohibición del derecho (definición nominal) y antijurídica es una conducta que está en contradicción con el derecho (definición real)[84].

Si bien, de la definición anteriormente señalada podemos decir que en el delito de Acceso ilícito a sistemas y equipos de informática la antijuridicidad aplica, cuando el sujeto activo accede con o sin autorización a algún sistema o equipo de informática causando en el sistema o equipo, un daño a la información.

Por su parte, Edmund Mezger en su obra Derecho Penal parte general, nos explica el elemento de la culpabilidad al decir que, es el conjunto de los presupuestos que fundamentan el reproche personal al autor por el hecho punible que ha cometido[85].

La culpabilidad en el delito de Acceso ilícito a sistemas y equipos de informática se traduce, cuando al sujeto activo se le imputa el hecho típico y antijurídico con el juicio de reproche por la conducta ilícita que ha cometido, transgrediendo así las leyes penales.

Por lo tanto, podemos señalar, que si en un hecho cometido por una persona falta alguno de estos elementos integrantes del delito (acción u omisión, tipicidad, antijuridicidad o culpabilidad) en la conducta, ésta misma, no se puede constituir como delito, por lo tanto no se puede reprochar.

Ahora bien, después de haber analizado el concepto de delito así como también sus elementos positivos encuadrados al delito de acceso licito a sistemas y equipos de informática, podemos decir que su estudio es importante para precisar las conductas que actualmente han surgido en este mundo globalizado, y asimismo insistimos en que la ley debe de estar al día con las nuevas conductas ilícitas del fenómeno antijurídico de cibercriminalidad denominadas también como delitos informáticos.

---

[84] Mayer, Max Ernst, *Derecho penal parte general,* trad. Sergio Politoff Lifschitz, Argentina, editorial B de F, 2007, p.217 y 218.
[85] Mezger, Edmund, *Derecho penal parte general,* 2a. ed., México, Cárdenas Editor y Distribuidor, 1990, p. 189.

## I. CONCEPTO DE DELITO INFORMÁTICO

Aunque en el Código Penal Federal (C.P.F) no se establece el tipo penal descrito como delitos informáticos, ni en un título propio, ni en ningún capítulo, aun así abordaremos su concepto, porque el delito de acceso ilícito a equipos y sistemas informáticos, está reconocido por la doctrina jurídica como el llamado delito informático, y en algunos códigos penales estatales si se encuentra como tipo penal (como lo veremos más adelante).

Estas conductas delictivas han sido denominadas como delitos informáticos o ciberdelitos por la ONU y por la doctrina jurídica, también son atendidas en el aspecto de la investigación por parte de la informática forense describiéndolas como cibercriminalidad o cibercrimen.

Palazzi manifiesta que debe señalarse, por lo demás que el concepto de delito informático ha ido evolucionando con el tiempo y en relación a los avances tecnológicos. Así, Sieber Ulrich señala que los primeros casos de delitos informáticos datan en la década de los setenta.[86].

Así pues, el concepto de delito informático se ha ido estructurando conforme a los años, tomando en cuenta la evolución de los equipos, sistemas informáticos, sistemas operativos y redes, los cuales son el medio comisivo de estas conductas o bien, son también el objeto sobre el cual recae la conducta.

En 1983 un grupo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) definió al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos[87].

La organización mundial OCDE fue una de las primeras que denominó a los delitos informáticos, el cual, esta conceptualización señala la intromisión de una

[86]Palazzi, Pablo Andrés, *Delitos informáticos,* Argentina, AD-HOC editores, 2000, p. 37.
[87] *Idem,* p. 39.

conducta ilícita en los sistemas y equipos informáticos con el objeto de ocasionar daños a la información contenida en ellos.

Para el autor Donn B. Parker, citado por Leyre Hernández Díaz en la obra Derecho penal informático refiere que este mismo, es uno de los primeros autores que conceptualiza al delito informático, el cual nos dice que es:

El delito informático, como abuso informático, es, cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionalmente, obtuvo o pudo haber obtenido un beneficio[88].

Siendo la anterior, una de las primeras conceptualizaciones del delito informático, ésta, es muy vaga, pues no define con exactitud la precisión de lo que conlleva la conducta informática delictiva, y se olvida de señalar que el ciberdelito también comprende a las computadoras sistemas o redes como objeto del mismo.

Sin embargo el autor toca un punto muy importante en esta conceptualización, al señalar que por los medios informáticos se dañan bienes jurídicos fundamentales, pero, no menciona con exactitud cual o cuales son estos bienes jurídicos que se afectan en la ejecución de éste.

Julio Téllez Valdés nos señala el concepto de delito informático al definirlo en dos vertientes como concepto atípico y típico:

Los delitos informáticos son actitudes contrarias a los intereses de las personas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)[89].

Este autor señala el concepto de típico del delito informático atendiendo que estas conductas ilícitas que de él se desprenden están reguladas y sancionadas por

[88]Hernández Díaz, Leyre, "Aproximación conceptual de derecho penal informático", en Mata Barranco de la, Norberto J. (Coord.), *Derecho penal informático,* España, Editorial Aranzadi, 2010, p. 36

[89] Téllez Valdez, Julio, *op. cit.,* p. 187.

la norma jurídico penal tanto en el C.P.F como en los Códigos penales de los estados del país.

Por otra parte, también en su conceptualización manifiesta que existen conductas ilícitas que son ejecutadas por medio de la informática como instrumento o fin, que afectan bienes jurídicos de las personas, y que no se encuentran tipificadas por la ley penal.

Atendiendo a las conceptualizaciones anteriormente señaladas por estos autores, podemos decir que un delito informático o ciberdelito implica conocer, copiar, obtener, modificar, destruir, provocar pérdida y/o apoderamiento de información total o parcial, alterando o dañando el sistema operativo de cómputo o red.

La conducta informática ilícita se puede comisionar diversas variantes que implican el usar, entrar, interceptar, interferir, o agredir, a una computadora, Red o sistema informático, con o sin la autorización, afectando el bien jurídico de la información contenida en estos mismos.

Este fenómeno de conductas ilícitas y antijurídicas, implican desde acceder con o sin autorización a sistemas informáticos, para actuar en contra de la información contenida, haciendo que la conducta y los efectos recaigan directamente sobre sí mismos, o bien, que éstos, sirvan de apoyo como medio o instrumento fundamental para llevar a cabo el ilícito y cometer el fin específico.

Asimismo, Leyre Hernández Díaz nos dice que no se puede hablar de un delito informático, sino de una pluralidad de ellos, en los que la única nota en común es su vinculación de alguna manera con los ordenadores, ni la forma de comisión del hecho presenta siempre características semejantes[90].

De esta manera, podemos observar que el concepto de delito informático comprende un solo delito, pero a la vez, este se conforma de una pluralidad de conductas informáticas ilícitas, como lo afirma Leyre Hernández, a la vez son las

[90] Hernández Díaz, Leyre, *op. cit.,* p. 40.

diferentes modalidades con las que se puede comisionar este delito, que parten de los sistemas informáticos conformándose así los ciberdelitos tipificados por la ley.

## II. TIPIFICACIÓN DE LAS CONDUCTAS DELICTIVAS INFORMÁTICAS EN MÉXICO

Atendiendo dogmáticamente al fenómeno de los delitos informáticos, estos se encuentran regulados por el Derecho Penal Positivo, en el que se han introducido las figuras típicas de la informática en los Códigos Penales del país tanto de orden federal como del fuero común.

Por ello, procederemos a interpretar la ley penal para desentrañar su sentido, determinar cuáles son las limitaciones y los alcances que plasma el legislador en el texto de la ley; cuál es el bien jurídico que tutela, de qué manera se protege y a qué sujetos protege.

### 1. *Código Penal Federal*

El delito de Acceso ilícito a sistemas y equipos informáticos se encuentra tipificado por el Código Penal Federal vigente en los artículos 211 bis 1 al 211 bis 7, correspondientes al Título Noveno denominado Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

De esta manera, Molina Salgado apunta que, la legislación penal pretende asociar o de alguna forma tratar a la revelación de secretos como delitos informáticos, por el hecho de incluir este ilícito en el mismo capítulo en el que se contemplan otros ilícitos relacionados con la informática[91].

Así pues, en un análisis exhaustivo de los artículos antes mencionados, podemos mencionar que estos se centran a proteger la información contenida en los equipos y sistemas informáticos, protegidos por algún mecanismo de seguridad de personas físicas o morales, los del Estado, y los que se encuentran en las instituciones que integran el sector financiero del país.

[91] Molina Salgado, Jesús Antonio, *Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial,* México, Porrúa, 2003, P.25.

Por consiguiente, en primer lugar se encuentran protegidos los equipos y sistemas de cómputo pertenecientes a las personas físicas y morales, utilizados en el ámbito personal o empresarial en sus actividades diarias ya sea de carácter público o privado (protegidos por el artículo 211 bis 1).

Este artículo regula la conducta ilícita, cuando una persona sin autorización acceda a éstos para causar modificación, provocar perdida de información contenida en los mismos, sancionándolos con seis meses a dos años de prisión y con cien a trescientos días multa.

Por otro lado, también se comprende al acceso ilícito a éstos con el objetivo de conocer (penetrar en el sistema o equipo informático sin causar daño) o copiar información, a esto se sancionará con una penalidad más baja que la anterior, que será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

En segundo lugar se encuentran protegidos los propios del Estado, estos vienen siendo los equipos y sistemas de cómputo, y Redes pertenecientes al Estado instalados, que operan en oficinas de gobierno, los sistemas del e-México y e-conectado (contemplados en los artículos 211 bis 2 y 211 bis 3 del C.P.F).

Asimismo, el artículo 211 bis 2 se encarga de tipificar a todo aquel que sin autorización modifique, destruya o provoque perdida de información contenida en estos sistemas y equipos informáticos del Estado, a lo que se le suma en el párrafo segundo las conductas de conocer y copiar información.

Por su parte, el artículo 211 bis 3 protege la información contenida en sistemas y equipos informáticos pertenecientes al Estado que se utilicen en materia de seguridad pública, para las conductas de acceso autorizado que indebidamente obtengan, copien o utilicen la información que se contengan.

Y en tercer lugar, en los artículos 211 bis 4 al 211 bis 6, se encuentran protegidos los equipos y sistemas de cómputo pertenecientes a las instituciones que integran el sistema financiero de nuestro país; estas son: Banco de México, Secretaria de Hacienda y Crédito Público (SHCP), Comisión Nacional Bancaria y de

Valores (CNBV) y la Secretaria de Administración Tributaria, entre otras Instituciones más.

Primeramente, el artículo 211 bis 4 regula el acceso sin autorización a estos equipos, sistemas de cómputo o redes con el objeto de modificar, destruir o provocar pérdida de información en ellos otorgándoles una penalidad de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Por el contrario, el artículo 211 bis 5 atiende la conducta ilícita de acceso con autorización a los sistemas y equipos informáticos que integran el sector financiero, por ende, una persona que tiene la autorización es porque es un servidor público o un empleado directo o indirecto; otorgando una penalidad de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

El último párrafo de este artículo, contempla una agravante para las penalidades previstas por este mismo, incrementándolas hasta en una mitad más, si la conducta ilícita la cometieron funcionarios públicos o empleados de las instituciones que integran el sector financiero.

Por su parte el artículo 211 bis 6 refiere que para los efectos del artículo 211 bis 4 y 211 bis 5, se entiende por instituciones que integran el sector financiero las señaladas por el artículo 400 bis del C.P.F; remitiéndonos al numeral 400 bis de este mismo ordenamiento jurídico no encontramos textualmente cuales son dichas instituciones.

Por último, el artículo 211 bis 7 establece una agravante para todas las penalidades anteriormente descritas hasta una mitad más, cuando la información que se obtenga del acceso ilícito a estos sistemas informáticos se utilice en provecho propio o ajeno.

Por ende, todos los equipos, sistemas informáticos o Redes anteriormente descritos, ya sea de particulares, del Estado o los que se encuentran en las instituciones que integran el sector financiero están propensos a ser víctimas de algún acceso ilícito provocando un delito, es por ello que se encuentran regulados por la ley.

Así pues, después de haber analizado los artículos anteriores, se aprecia que el C.P.F tipifica al delito de Acceso ilícito a sistemas y equipos de informática resguardando este bien jurídico para que no sea atentado, y de ser así esta conducta ilícita tenga su consecuencia jurídica.

2. *Códigos Penales Estatales*

De la misma manera al Código Penal Federal, las conductas informáticas ilícitas que atentan en contra de los sistemas informáticos han sido tipificadas por diferentes códigos penales de los estados, algunos muestran similitudes al ordenamiento jurídico Federal y otros los tipifican de forma muy distinta.

Unos son tipificados en los capítulos de Revelación de secretos y acceso ilícito a sistemas y equipos informáticos, otros en capítulos de delitos contra la seguridad pública, delitos contra la fe pública, delitos contra la seguridad de medios informáticos, fraude, contra el patrimonio y otros en capítulos denominados como delitos informáticos.

En este sentido, podemos notar que los tipos penales son muy variados, en los cuales, en unos estados se encuentran en títulos donde no están en concordancia con el Código Penal Federal, por lo que en sus congresos estatales manejan una técnica legislativa diferente.

Luego entonces, para abordar este tema de la mejor manera, primero señalaremos aquellas entidades federativas que regulan el tipo penal como acceso ilícito a sistemas y equipos de informática, los cuales se equiparan a lo contemplado por el C.P.F.

Posteriormente procederemos a señalar aquellos estados que tipifican el Acceso ilícito a sistemas y equipos de informática pero de manera diferente, tanto en sus tipos penales como en sus títulos y capítulos, para comparar las legislaciones de este tipo de delito.

Y por último, señalaremos los estados del país que carecen de legislación en sus códigos penales estatales para este tipo de conductas delictivas que se

desprenden de la informática para causar daño, de las cuales, se necesita que sus legisladores las tipifiquen.

Asimismo, los estados que equiparan a la legislación contemplada por el C.P.F son, Baja California, Chiapas, Jalisco, Querétaro, y Tamaulipas que tipifican estas conductas mediante al título denominado Revelación de secretos, con el tipo penal de Acceso ilícito a sistemas y equipos de informática.

Por otra parte, el estado de Tabasco muestra similitud con el C.P.F al contemplar este delito como acceso ilícito a sistemas y equipos de informática, pero lo regula en el titulo denominado como delitos contra la autenticidad o la veracidad documental (en los artículos 326, 326 bis1 y 326 bis 2), por lo que se ausenta un poco de la legislación federal.

Por ende, aquí se aprecia que el estado de Tabasco da un tratamiento distinto a lo contemplado por el C.P.F al cambiar el título donde se contempla el tipo penal, sin embargo su contenido es muy similar al ordenamiento federal pues el tipo penal es el mismo.

De forma similar, el estado de Chihuahua tipifica el acceso ilícito a sistemas y equipos informáticos, pero lo contempla en el titulo denominado delitos contra la seguridad y el normal funcionamiento de las vías de comunicación y los medios de transporte contemplado en los artículos 237 bis al 237 bis quinquies.

Por otro lado, los estados de Sonora, Oaxaca y Yucatán en los títulos denominados delitos contra la seguridad pública tipifican delito de acceso ilícito a sistemas y equipos informáticos, para quien aceda ilícitamente a solamente a las bases de los sistemas informáticos de sus Estados.

De manera similar a los grupo de los Estados anteriores, Coahuila tipifica el acceso ilícito a sistemas y equipos de informática, en el título de delitos contra la seguridad pública, pero este se extiende un poco más que los demás, al proteger también los equipos y sistemas informáticos de los particulares en el artículo 281 bis, y agrega una agravante en el artículo 281 bis 1 cuando el agente actué con fines de lucro y cuando sea un empleado de confianza.

Por otra parte, los estados de Hidalgo, México y Quintana Roo tipifican solamente el acceso ilícito a sistemas y equipo de cómputo pertenecientes a las instituciones bancarias, en capítulos denominados falsificación de documentos y usos de documentos falsos, por lo que dejan sin protección penal a los sistemas y equipos de informáticos de los particulares, de las personas físicas y los del Estado.

En cambio, los estados de Aguascalientes, y Guanajuato manejan tipos penales muy diferentes a los antes mencionados, por ejemplo Aguascalientes con el capítulo denominado tipos penales protectores de la confidencialidad, la intimidad de la información y la identidad de las personas; y Guanajuato en el capítulo de violación de correspondencia.

Por el contrario, los estados que tipifican estas conductas de acceso ilícito a sistemas y equipos informáticos con el tipo penal denominado delitos informáticos, correspondientes a los títulos de delitos contra el patrimonio, son los estados de Morelos, Nayarit, Nuevo León, Puebla, Sinaloa, Zacatecas y Veracruz.

Cabe señalar que el estado de Sinaloa fue la primera entidad federativa del país en tipificar las figuras antijurídicas de la informática, mediante el Decreto número 539 publicado por el Periódico Oficial del Estado de Sinaloa con fecha de 28 de octubre de 1992, incorporando el articulo 217 al Código Penal para el Estado de Sinaloa, colocándolo en el titulo decimo denominado Delitos contra el patrimonio, capítulo V denominado Delito informático.

Estos estados se acercan a lo descrito por la doctrina y por la Organización de las Naciones Unidas al regular estas conductas delictivas en sus tipos penales como delitos informáticos, por lo que se alejan de lo contemplado por el Código Penal Federal, pero a la vez extienden los elementos descriptivos de las conductas.

Asimismo, el estado de Morelos en el artículo 148 quarter, y el estado de Sinaloa en el artículo 217, de sus códigos penales estatales, tipifican el delito informático de manera muy similar, al señalar que este tipo de delito es de carácter doloso al que use, entre, intercepte, interfiera, altere o dañe una base de datos, además contemplan la conducta del fraude informático.

El cambio, el estado de Puebla tipifica el acceso ilícito a sistemas y equipos informática en su capítulo denominado delitos informáticos, correspondientes a los artículos 475, 476, 477, 478, siendo estos, los últimos del Código penal para el estado, adicionados el 30 de diciembre de 2013.

De igual manera, los estados de Nayarit, Nuevo León, Zacatecas y Veracruz protegen el bien jurídico correspondiente a la privacidad y la intimidad de la información contenida en sistemas y equipos informáticos para quien acceda ilícitamente a éstos con el propósito de causarle daño a su contenido.

De forma muy similar a los estados de Morelos, Nayarit, Nuevo León, Puebla, Sinaloa, Zacatecas y Veracruz, el estado de Tlaxcala tipifica el acceso ilícito a los sistemas y equipos informáticos en el titulo denominado delitos contra la seguridad en los medios informáticos, en los artículos 316 al 320 de su código penal.

Por el contrario, los estados de Colima, Baja California Sur, Durango, y Guerrero, tipifican el acceso ilícito a sistemas informáticos pero solo los pertenecientes a las instituciones bancarias, en los títulos de delitos contra el patrimonio en sus capítulos correspondientes al delito de fraude.

En Colima el artículo 201 fracción VII correspondiente a la manipulación informática; Baja California sur en el artículo 363 y 364; Durango en los artículos 425 y 426 con la descripción de quien para obtener algún lucro para sí o para un tercero, por cualquier medio acceda, entre o se introduzca en los sistemas financieros; y de igual manera Guerrero en los artículos 237 y 238.

Por otra parte, los estados de Campeche, Michoacán y San Luis Potosí no refieren tipificación alguna en sus Códigos Penales Estatales sobre este tipo de delitos, tampoco tienen ninguna ley estatal que los tipifique, por lo que dejan sin protección alguna a este bien jurídico.

Así pues, el análisis dogmático del delito de Acceso ilícito a sistemas y equipos informáticos por los estados del país, podemos ver que la mayoría de ellos, no muestran una homologación con lo estipulado en el C.P.F., por lo que presentan en sus tipos penales una técnica legislativa distinta.

## III. JUSTIFICACIÓN DE LA TIPIFICACIÓN DE LAS CONDUCTAS DELICTIVAS INFORMÁTICAS EN EL CÓDIGO PENAL FEDERAL

Las conductas que atentan contra los sistemas informáticos, hoy en día son más comunes de lo que se cree, sin embargo su tipificación en la mayoría de las legislaciones es confusa desde el punto de vista de la técnica legislativa y de la teoría del delito.

Estas figuras delictivas que se han ido impregnado en los diferentes equipos informáticos que utilizamos con bastante recurrencia, han ido afectando bienes jurídicos importantes de las personas tanto físicas como morales, e inclusive también del Estado, por consiguiente también a la misma sociedad.

Ahora procederemos a analizar las cuestiones encaminadas a la justificación del por qué estas conductas ilícitas están tipificadas como delito en el Código Penal Federal, mostrando el objetivo que tienen; en toda norma jurídica penal el bien jurídico se convierte en el principal elemento.

Para lo anterior, primero daremos a señalar el concepto de bien jurídico, el cual, Malo Camacho lo define como el objeto de la protección de un concreto interés social, individual o colectivo reconocido y protegido por el Estado a través de la ley penal[92].

Así pues, para el autor encinta el bien jurídico es un ente protegido por las normas jurídico penales, las cuales, los sujetos de esos bienes jurídicos son las personas tanto físicas como morales, el Estado y a lo que se le suma también la misma sociedad. En otras palabras el bien jurídico es el interés vital reconocido por el legislador en el texto de la ley, en la creación del tipo penal.

> El concepto de bien jurídico debe limitar al legislador en el momento de crear tipos penales y de establecer la sanción penal de comportamientos; además, ha de obligarlo a que busque los bienes jurídicos no fuera de la realidad

[92] Malo Camacho, Gustavo, *Derecho penal mexicano,* 7a. ed., México, Porrúa, 2013, p. 280.

naturalística, ni dentro de la valoración subjetivo-moral, sino exclusivamente en el ámbito de la dañosidad social[93].

Asimismo, el legislador en el texto de la ley debe de plasmar primordialmente la esencia del bien jurídico que se intenta proteger con la creación de la ley penal, tomando en cuenta como se afecta este mismo describiendo la conducta típica y creando el delito, a parir de ello, procederá a determinar las sanciones que se considere más pertinentes ante la violación de estos bienes jurídicos.

> Los bienes jurídicos tienen como fundamento valores culturales que se basan en las necesidades individuales. Estas se convierten en valores culturales cuando son socialmente dominantes. Y los valores culturales se transforman en bienes jurídicos cuando la confianza en su existencia surge necesitada de protección jurídica[94].

Los bienes jurídicos se encuentran en la naturaleza de los sujetos pasivos como una parte inherente de ellos, se constituyen primeramente como un carácter que adquiere valor dentro de una sociedad, de la que posteriormente se conforman como bienes jurídicos protegidos por el Estado, cuando éste, los plasma en los ordenamientos jurídicos.

Luego entonces, Malo Camacho nos dice que para el autor Lizt los bienes jurídicos están más allá del ordenamiento jurídico, y entiende, así, que los mismos surgen y están en la vida y por eso el derecho debe de protegerlos[95].

Lizt destaca un punto importante, al precisar que los bienes jurídicos se encuentran inherentes al ser humano, independientemente de si están o no plasmados en una ley, pero a la vez, nos afirma, que es obligación del Estado buscar su protección con los ordenamientos jurídicos conformándolos como tipos penales.

---

[93] González-Salas Campos, Raúl, *La teoría del bien jurídico en el derecho penal,* 2a. ed., México, Oxford, 2001, P. 48.

[94] Regis Prado, Luiz, *Bien jurídico y constitución,* trad. de Luis Enrique Álvarez Aranda, Perú, Ara editores, 2010, p. 44.

[95] Malo Camacho, *op. cit.,* p. 284.

> Bettiiot comentado por Jiménez Huerta señala que: la importancia del tipo legal no consiste tanto en la interpretación del principio fundamental *nullun crimen sine lege*, sobre el que todos los juristas están de acuerdo (un hecho que no se adecúa perfectamente a un tipo delictivo no puede ser susceptible de valoración penal), sino más bien en la función metodológica que él ofrece a los fines de la exposición y sistematización de las especies delictivas[96].

Esa función que comenta Bettiiot, da a contrastar que el tipo penal describe la conducta ilícita del delito establecido en la ley penal, por consiguiente, si la conducta antisocial cometida no concuerda exactamente con lo estipulado en la ley penal, esa conducta no puede ser reprochada como delito.

De esta forma, todos los tipos legales regulados por el derecho penal se configuran exclusivamente para proteger bienes jurídicos y no ideologías políticas, ni valores meramente éticos, culturales o morales, que no implican una nocividad social[97].

Asimismo, podemos decir que en los códigos penales se encuentran los tipos penales encaminados a proteger los bienes jurídicos de las personas y del Estado tales como lo son la vida, la libertad, la integridad, la libertad sexual, el patrimonio, la intimidad, la privacidad, la información, la salud, la moral pública, seguridad pública y el bien jurídico de la paz y la seguridad de las personas.

Por ello, el 13 de noviembre de 1998, se expusieron motivos legislativos al H. Congreso de la Unión para proteger los bienes jurídicos correspondientes a la intimidad y la privacidad de la información contenida en los sistemas y equipos informáticos.

En esta exposición de motivos se reconoce que el uso de la tecnología informática es un instrumento que facilita a la sociedad en su desarrollo económico y cultural, al ser utilizada en todas las áreas del desarrollo social de una nación, así

---

[96] Jiménez huerta, Mariano, *Derecho penal mexicano,* 2a ed., México, Porrúa, 1977, t. I, p. 67.
[97] González-Salas Campos, Raúl, *op. cit.,* p. 59.

como también se reconoce un incremento de personas que tienen acceso a ésta tecnología.

Debido al avance tecnológico que el Estado mexicano presentó en los últimos años, se expone que, paralelamente a él, han surgido nuevas formas de conducta antisocial que han hecho de los equipos y sistemas informáticos instrumentos para delinquir como el objeto o el fin en sí mismo de la infracción.

En el contexto internacional la ONU instó a los Estados miembros (México incluido) a intensificar esfuerzos para combatir este tipo de conductas mediante la creación de nuevos tipos penales y procedimientos de investigación para hacer frente a estas nuevas y sofisticadas formas de actividad criminal.

Se menciona que la Unión Europea tiene una legislación muy completa en el campo cibernético, que incluye seguridad de datos, defraudación cibernética entre otras disposiciones más, por otra parte Alemania, Austria y Francia tienen una ley específica para combatir los delitos informáticos, en tanto que Argentina, España y Estados Unidos los tipifican en sus Códigos Penales.

Debido a lo anterior, en esta exposición de motivos se expresa que el Estado mexicano está obligado a proteger los bienes jurídicos de las personas que utilizan la informática como instrumento de desarrollo, por ello requieren de un marco jurídico acorde al avance tecnológico existente, debido a que México carece de estos tipos penales.

A lo que se le suma, la postura de establecer la protección de la privacidad e integridad de la información contenida en sistemas y equipos de cómputo, de almacenamiento o procesamiento de información en los ordenamientos jurídicos penales.

Por ello, la iniciativa del Ejecutivo Federal propone adicionar al Código Penal Federal un capitulo para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad con el propósito de conocer, copiar, modificar, o provocar perdida de información que en ellos se contenga.

Conforme esta exposición de motivos se establece que el bien jurídico que se pretende tutelar es la privacidad y la integridad de la información. Se incluyen estos nuevos tipos penales en el Titulo Noveno del Código Penal Federal denominado Revelación de secretos.

Por otra parte, también en esta iniciativa presentada por el Ejecutivo Federal se propuso establecer una punibilidad mayor cuando las conductas sean cometidas en contra del Estado, debido a que este mismo utiliza los sistemas de cómputo, computadoras, bases de datos y programas informáticos para el almacenamiento y procesamiento de información los que se constituyen como informática jurídica.

Asimismo, también se propuso establecer ordenamientos jurídicos correspondientes para proteger la información contenida en los sistemas y equipos de cómputo pertenecientes a las instituciones que integran el sector financiero, debido éstas han sido afectadas por la comisión de estas conductas. Por último, se propuso agravar las sanciones previstas para los tipos penales antes descritos, cuando con la comisión de dichos ilícitos se obtenga un provecho propio o ajeno.

Conforme a la exposición de motivos y a la iniciativa antes señaladas, estos tipos penales fueron adicionados al Código Penal Federal en los artículos 211 bis 1 al 211 bis 7, publicados en el Diario Oficial de la Federación de tomo DXLVIII, Número 10, de fecha lunes 17 de mayo de 1999, los que entraron en vigor al día siguiente de su publicación.

Asimismo, estos artículos una vez incorporados al Código Penal, son correspondientes al capítulo II, Título Noveno del libro segundo, el cual fue reformada por adición su denominación sustentándose como Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

La protección a la privacidad e integridad de la información contenida en los sistemas y equipos informáticos es un bien jurídico fundamental y tutelado que tienen todos los ciudadanos, por lo que son protegidos por los tipos penales consagrados en los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal.

Pedro López Calvo señala que, una de las preocupaciones de esta época de alta tecnología es la inseguridad en los sistemas electrónicos y automáticos de información tanto de nivel estatal como empresarial, desde la globalización del sistema interbancario y de Internet[98].

A raíz de brindarle protección a la información contenida en los equipos y sistemas informáticos se tipifican estas conductas ilícitas estableciéndolas en los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal con el objeto frenar la inseguridad de la privacidad de la información contenida en estos equipos.

Asimismo surgen nuevas amenazas a la información como es el caso de los virus informáticos y los programas dirigidos con un fin determinado, con los que la información puede ser sustraída, borrada, vendida, conocida en forma ilegal, esta información en los últimos años se le trata como una mercancía [99].

Como la información es un factor de gran importancia que adquiere valor pecuniario; principalmente aquella pertenecientes a empresas, instituciones bancarias y del Estado, esta, le puede dar al sujeto activo elevadas sumas de dinero a su favor, y grandes pérdidas para la víctima.

## IV. EVOLUCIÓN Y DESARROLLO DE LAS FIGURAS TÍPICAS DE LA INFORMÁTICA EN EL CÓDIGO PENAL FEDERAL

La privacidad y a la intimidad de la información contenida en los equipos y sistemas informáticos es un bien jurídico, afectado por una nueva serie de conductas antisociales desprendidas de los sistemas informáticos para atentar en contra de estos mismos.

Si bien podemos notar que la tecnología informática avanza más rápido que las legislaciones del derecho, en esta vertiente, el derecho penal positivo atiende

[98] López Calvo, Pedro, *Derechos humanos, victimología, terrorismo y sus diversas modalidades delictivas, secuestros, delitos informáticos y armas de destrucción masiva,* México, editorial Flores, 2015, p. 408.
[99] Palazzi, Pablo Andrés, *op. cit.,* p. 44.

tipificando estas figuras delictivas de forma dogmática en atención al fenómeno de nuevas conductas que parte de los sistemas informáticos.

En la medida que va evolucionando las tecnologías informáticas van innovando nuevas formas de delinquir, es aquí, cuando también se deben de ir reformando las legislaciones penales procedentes a esta clase de delitos para tomar en cuenta las nuevas formas de delinquir.

En el sentido que el delito de Acceso ilícito a los sistemas y equipos informáticos se encuentra tipificado por el C.P.F en los artículos 211 bis 1 al 211 bis 7, como ya se mencionó anteriormente, es considerable señalar ahora las reformas que han tenido estos mismos, así como también sus exposiciones de motivos que le dieron origen.

Conforme a lo anterior cabe señalar que una reforma legislativa es el cambio o modificación de un ordenamiento jurídico, con el objetivo de mejorar las situaciones previstas, o que no hayan sido previstas desde el inicio, o bien, adecuar el marco jurídico a las nuevas condiciones de la sociedad en atención al avance de la informática.

Las reformas tecnológicas actuales exigen un profundo análisis y desarrollo de las instituciones jurídicas existentes, así como una participación activa de los juristas y profesionales de todas las ciencias involucradas, para regular las consecuencias del auge informático contemporáneo[100].

Asimismo procederemos a analizar las diferentes reformas legislativas que han tenido los artículos (211 bis 1 al 211 bis 7) procedentes al delito informático, para conocer en qué medida ha avanzado el derecho desde la incorporación de estos tipos penales.

El 24 de junio de 2009 por el tomo DCLXIX, número 18 del Diario Oficial de la Federación se dio a conocer que estos artículos tuvieron su primera modificación en el texto de la ley, en la cual, se adicionan los párrafos terceros de los artículos

[100] Cardeño Shaadi, José Ramón, *Las patentes de software,* México, Porrúa, 2013, P. 4.

211 bis 2 y 211 bis 3, con el objeto de prever condiciones que no se habían contemplado desde su creación en el año de 1999.

Las mencionadas reformas tuvieron lugar por la exposición de motivos de fecha de 2 de octubre de 2008, con la Iniciativa del Ejecutivo presentada el 30 de septiembre de 2008 a la cámara de diputados, del H. Congreso de la Unión, la cual nos dice que:

Es fundamental proteger a la información contenida en los sistemas y equipos informáticos que se utilicen en materia de seguridad pública, tales como el Sistema Único de Información Criminal, el Registro Nacional de Personal de Seguridad Publica, el Registro Nacional de Armamento y Equipo y la Estadística de Seguridad Publica como partes integrantes de la Plataforma de México.

Dicha plataforma proporciona a las instituciones de seguridad pública de los tres niveles de gobierno la información precisa y constante en materia de seguridad pública, que generan la inteligencia apta para el ejercicio de las atribuciones que tienen encomendadas.

Debido a ello es que se reforma el artículo 211 bis 2 en el que se adiciona el párrafo tercero, que conlleva a regular el acceso sin autorización de cualquier persona a equipos y sistemas de cómputo de la seguridad pública, que tengan el fin de conocer, obtener, copiar, o utilizar la información contenida en esos equipos de la seguridad pública.

En esta misma reforma también viene a regular sanciones para aquellos servidores públicos que sean el sujeto activo del delito informático, otorgándoles la destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

El objeto de esta reforma es sancionar a los servidores públicos que abusen de su cargo ya son ellos quienes tienen fácil acceso a las bases de datos de los sistemas informáticos de las instituciones pertenecientes al Estado, por lo que son sujetos en calidad de garante del uso adecuado de la informática del Estado, en

donde se maneja información en riesgo de la seguridad nacional de carácter sensible del mismo y también de los propios ciudadanos.

De la misma manera se reforma el artículo 211 bis 3 en la que se adiciona el párrafo tercero, prevé la misma regulación que la anterior, pero, para las personas que si tengan autorizado el acceso a equipos y sistemas informáticos en materia de seguridad publica estableciendo igual punibilidad.

En el mismo sentido, esta reforma agrega una agravante para los servidores públicos que si tengan autorizado el acceso a estos sistemas informáticos y que delincan, al señalar una sanción de hasta más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Por otra parte, la más reciente modificación que han tenido estos artículos fue con fecha de 17 de junio de 2016, por el tomo DCCLIII, número 15 del Diario Oficial de la Federación, en la cual, se adiciona el último párrafo del artículo 211 bis 2 con el objetivo de resguardar a los equipos y sistemas informáticos que se encuentran en los organismos impartidores de justicia.

Dicha reforma fue propuesta el 9 de diciembre de 2014 con la exposición de motivos que dice: se añade una gravante con lo que se pretende salvaguardar los registros de procedimiento penal que serán resguardados mediante sistemas informáticos.

Esta agravante incorpora la duplicidad de la penalidad establecida para aquel, en el que la conducta obstruya, entorpezca, obstaculice, limite, o imposibilite la procuración o la impartición de justicia o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Con esta agravante la punibilidad aumenta de dos a ocho años de prisión y de cuatrocientos a seiscientos días multa (equivalente de $32,016 a $96,048 pesos) para la persona que sin autorización modifique, destruya o provoque perdida de información en sistemas o equipos de informática del Estado que imposibilite la procuración o la impartición de justicia.

De la misma manera, si el sujeto activo es o hubiere sido un servidor público la penalidad seria de ocho a veinte años de prisión y de mil a dos mil días multa de salario mínimo vigente en la Ciudad de México equivalente de $80,040 a $160,080 pesos; esto, porque ellos tienen las facilidades de acceder a los sistemas informáticos que se utilizan en las tareas de procuración e impartición de justicia penal.

Conforme al anterior análisis de reformas procedentes a estos artículos, podemos ver que éstos presentan aun deficiencias, pues la generalidad del lenguaje legislativo es muy vaga y ambigua a los tipos penales, por lo que todavía se tiene que seguir trabajando en precisar las conductas antijurídicas dela informática, así como también sus modalidades para proporcionar certeza jurídica al destinatario de la norma.

Las conductas que afectan a éste bien jurídico son variadas, estas pueden ser el acceso ilícito a sistemas y equipos de informática, sabotaje informático, virus informáticos, gusanos informáticos, bomba lógica o cronológica, caballos de Troya, robo de información, manipulación informática, piratería informática, *hacking* y, *craking,* (las que definiremos en el siguiente subtema).

Esas conductas son denominadas como delitos informáticos por la doctrina jurídica, actúan de diferente manera cada una, que conllevan a afectar la información contenida el sistema o equipo informático, causando un daño que puede ser total o parcial, e inclusive en algunas ocasiones provocan un daño irreparable.

## V. DIVERSAS CONDUCTAS CON LAS QUE SE PUEDE AFECTAR EL BIEN JURÍDICO DE LA INFORMACIÓN Y LA FORMA EN LA QUE ESTAS SE EJECUTAN

Como ya se mencionó en el concepto de delito informático, el tipo penal del delito de Acceso ilícito a sistemas y equipos informáticos se manifiesta con una pluralidad de conductas ilícitas informáticas diferentes, es decir, en su forma de comisión no constituye a ser siempre de la misma manera.

Por ello, en este tema precisaremos la definición de las diferentes formas de acceder a un equipo o sistema informático afectando la información contenida en él, a lo que le sumaremos la descripción y el análisis de cómo se ejecutan cada una de estas mismas, diferenciándolas unas de otras. Para una clara precisión del contenido de las diferentes modalidades informáticas ilícitas comenzaremos por definir la palabra definir:

Para el Diccionario de la Real Academia Española la palabra definir significa: fijar con claridad, exactitud y precisión el significado de una palabra o la naturaleza de una persona o cosa[101].

Así pues la palabra a nuestro criterio la palabra definir significa: precisar, especificar, determinar, concretar, decretar, puntualizar, delimitar, o esclarecer las características y/o cualidades de una persona o cosa con el fin de diferenciarla de las demás.

Por su parte Manuel Atienza nos dice que definir, en principio, es una operación mediante la cual se describe, se especifica, se aclara, o se establece el significado de una expresión lingüística[102].

De esta manera, comenzaremos por definir cada una de las modalidades en que se pueden presentar los delitos informáticos describiendo específicamente su concepto, precisando algunas de las características más esenciales y señalando como se ejecutan éstas mismas.

1. *Acceso no autorizado a sistemas o equipos informáticos*

López calvo cita a Oliver Hace, quien dice que, un acceso no autorizado, es la conducta de un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo, o hace la conexión por accidente pero decide voluntariamente mantenerse conectado[103].

[101] https://dle.rae.es/?id=C2rVUUs
[102] Atienza, Manuel, *El sentido del derecho,* España, Ariel editores, 2001, p. 52.
[103] López Calvo, Pedro*, op. cit.,* p. 431.

Esta conducta ilícita de acceder a un equipo o sistema informático constituye a ser un delito que afecta el secreto informático, pues con esa acción deliberada, se agrede a la información contenida en ellos, es decir, el sujeto activo con el sólo hecho de interceptar en el sistema informático, está conociendo la información contenida allí misma.

Al ejecutarse esta modalidad, la conducta ilícita informática, no sólo consiste en conocer la información, sino que el objetivo del sujeto activo podría ser también la de modificar, destruir o provocar perdida de información que se encuentre contenida en el sistema o equipo informático.

El ciberdelincuente ingresa sin autorización, a los datos que posee el directamente afectado, este ingreso puede son llevar a muchos agravantes, como el espionaje, la instalación de bombas lógicas, etc., o la simple acción de ingresar de manera no autorizada, como satisfacción o reto personal del hacker[104].

Además con la conducta de acceder sin autorización a un equipo o sistema informático sin previa autorización, el ciberdelincuente comisiona un delito, y puede ejecutarse en esa misma acción otro delito más, si así se corresponde a los objetivos que del sujeto activo.

2. *Sabotaje informático*

Es el acto de borrar, suprimir, o modificar sin autorización funciones o datos de la computadora con la intención de obstaculizar el funcionamiento normal del sistema las técnicas más comunes son los virus informáticos, los gusanos y las bombas lógicas o cronológicas[105].

El sabotaje informático comprende ser un delito que afecta el secreto informático de forma dolosa y particularmente grave, pues, con esta modalidad, el sujeto activo pretende eliminar la información contendida en el equipo provocando en la víctima la pérdida de ésta misma.

---

[104] *Ibídem,* p. 436.
[105]Villa, Escobosa, Jaime, "Los delitos informáticos", *op. cit.,* p.249.

El sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el *hardware* o en el *software* de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección[106].

Se dice que esta modalidad de delito es sofisticada porque, conforme se van mejorando los ordenadores, también de forma consecutiva, el delincuente informático busca nuevas maneras de sabotear el *hardware* o *software*, para así comisionar el ilícito.

De la misma manera, el sabotaje informático comprende a la conducta de hacerle daño al *hardware*, es decir, a la parte física de los ordenadores, pues si esta se destruye por medios informáticos, por consiguiente, también se le causa daño a la información contenida en él.

Por otra parte, si sabotaje informático se ejecuta para dañar el *software* del equipo (parte interna de los ordenadores que se encarga de almacenar y procesar información), la conducta ilícita va directamente encaminada a afectar a la información contenida en el mismo.

Cabe aclarar que el sabotaje informático no se debe de confundir con el tipo penal contemplado en el artículo 140 del Código Penal Federal que refiere al sabotaje como delito contra la seguridad de la nación, pues este es completamente diferente el bien jurídico que se protege, que es la seguridad interior del Estado.

3. *Virus informático*

Hidalgo Banilla cita a Sánchez Montufar quien define al virus informático como un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede multiplicarse y propagarse a otras computadoras[107].

---

[106] G. Salt, Marcos, "Los delitos informáticos de carácter económico" en J. Mailer, Julio B. (coord.), *Delitos no convencionales,* Argentina, Editores del Puerto, 1994, p. 229.
[107] Hidalgo Banilla, Antonio, *Derecho informático,* México, Flores Editor, 2013, Pp. 196 y 197.

Es decir, un virus informático es un programa informático maligno que tiene la característica de ser perjudicial, porque daña directamente a la información contenida en el equipo o sistema informático en el que se aloje, ocasionando así modificarla, destruirla o provocar pérdida de la misma.

A lo que se suma, que el virus informático tiene la habilidad de propagar su infección a otras computadoras con que se tenga contacto el virus, es decir, por medio de mecanismos de salida (memorias *USB*, unidades de *CD*, *Diskets,* entre otros) o por páginas web propagadas en la Internet.

> Asimismo, Sánchez Magro expresa que aunque históricamente los virus informáticos fueron bautizados por la prensa el 12 de octubre de 1985, con una publicación del New York Times, son conocidos como tales desde 1996, cuando fue acuñada esta denominación por Fred Cohen. Se aprovechan de los agujeros de seguridad que presentan los programas[108].

Efectivamente los virus informáticos se valen de un descuido de seguridad informática que tengan los equipos o sistemas informáticos, para adentrarse en ellos provocando su fin, es por eso que hay que tomar las medidas de seguridad informáticas adecuadas para así evitar ser víctima de este tipo de delito.

Por ello, se tiene que tener mucho cuidado en asegurar los equipos informáticos con un programa de antivirus, para que al momento de navegar en la red o de interceptar un mecanismo de salida en el equipo informático, éste no se infecte y evitar daños a la información contenida.

4. *Gusanos informáticos*

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos para modificar o destruir datos, pero es diferente al virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es benigno, mientras que el virus es un tumor maligno[109].

---

[108] Sánchez Magro, Andrés, "El ciberdelito y sus implicaciones procesales, en García Mexía, Pablo (coord.), *Principios de derecho de Internet,* España, Tirant lo Blanch, 2002, P. 273.
[109] Romero López, Lucero (coord.), *Jus informa TIC´s,* México, s.e., 2011, p. 189.

El gusano es un programa informático que se instala en los equipos o sistemas informáticos que puede causar gran daño a la información contenida en ellos, presenta características similares al virus informático, pero con éste no tiene la habilidad de reproducirse para seguir con sus fines.

Al no tener la capacidad de reconstruirse dentro del equipo o sistema informático, el gusano informático tampoco puede trasladarse hacia otros equipos informáticos para infectarlos, ésta es otra característica que lo diferencia del virus informático.

Como el gusano no tiene la habilidad para regenerarse, constituye que al momento en el que se encuentra su ubicación en el equipo o sistema informático, éste, se desactiva del sistema para destruirlo, pero, esto no quiere decir que se recupere la información a la que le causó daño.

Como el objetivo específico del gusano informático es modificar o destruir información contenida en el sistema o equipo informático, esto lo hace, que sea un delito que afecta el secreto informático, el que se encuentra tipificada la conducta ilícita por Código Penal Federal en los artículos 211 bis 1 al 211 bis 5.

5. *Bomba lógica o cronológica*

Norberto De la Mata y Leyre Díaz definen a las bombas lógicas como, rutinas introducidas en un programa para que al realizar una determinada acción, por ejemplo la copia del mismo, se produzcan alteraciones o daños en los programas o archivos al llegar a una fecha concreta o pasar un plazo de tiempo establecido[110].

La bomba lógica tiene un objetivo en particular, que consiste en pedir un rescate de carácter pecuniario por la información que tiene en su poder, es decir, es un secuestro de información, a cambio de no hacerle daño, mientras transcurre el tiempo en que se accione la bomba lógica en el sistema.

[110] Vázquez-Portomeñe Seijas, Fernando (Dir.), *Estudios penales criminológicos XXIX*, España, Universidad de Santiago de Compostela, 2009, p, 315.

Para su creación y funcionamiento requiere conocimientos especializados, toda vez que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro, a diferencia del virus o de los gusanos son difíciles de detectar antes de que exploten[111].

Para que se ejecute esta modalidad de delito informático se necesita que la bomba lógica o cronológica sea hecha por un experto en sistemas (sujeto cualificado), pues, sólo él la puede infiltrarla en el sistema y hacer que explote en el tiempo que le haya asignado.

6. *Caballos de Troya*

Son aplicativos infecciosos virtuales que requieren ser copiados e instalados manualmente en el ordenador o cerebro electrónico que será infectado, destruyendo la información que esté en el disco. Se presenta en un segmento de tiempo en el cual se activa y muestra su auténtico propósito[112].

Como el Caballo de Troya requiere que se instale manualmente en el equipo o sistema informático en el que se pretende afectar a la información contenida en el mismo, se necesita de una persona que tenga los conocimientos necesarios en el campo de la informática para instalarlo, lo que a la vez se comisiona un delito.

Esta modalidad de delito informático es diferente a las demás porque en ella, el programa maligno que destruye la información contenida en los sistemas informáticos, actúa de forma normal e inofensivamente como cualquier otro programa instalado en el equipo, pero una vez que se abre agrede a la información ocasionando su perdida.

7. *Robo de información*

El robo de información consiste cuando el sujeto activo accede con o sin autorización a un sistema o equipos informáticos con el objetivo de sustraer de ellos

[111] Medina Ortega, Cutberto Simón, *Contabilidad financiera jurídica y fiscal*, 2a ed., México, 7 editores, 2012, p.353.
[112] Paloma Parra, Luis Orlando, *op. cit.,* p. 42.

la información contenida en el mismo. Sin duda esta modalidad es realizada dolosamente.

> Hablando específicamente de los sistemas informáticos, dentro de estos se maneja a diario grandes cantidades de información de gran utilidad para el hombre, muchas de estas son de estricta confidencialidad y de gran importancia para algunas personas y otras son simplemente información que se quiere dar a conocer el público[113].

Debido a que en los sistemas informáticos se almacena y se procesa información, si esos sistemas son pertenecientes al Estado, forman parte de la informática jurídica, es en ellos donde se maneja información de carácter sensible, por eso que es susceptible a ser tipificada esta conducta de robo o apoderamiento de información.

El robo de datos en particular es un problema que aqueja actualmente a la sociedad ya que con frecuencia se apodera de información valiosa de manera ilegal utilizando precisamente estos sistemas de información y constituyen a una amenaza para la creación de una sociedad de la información que tenga seguridad[114].

Debido a lo anterior, es que se tipifica esta conducta de robo de información que se contenga en sistemas y equipos informáticos, como delito de Acceso ilícito a sistemas y equipos informáticos por los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal.

8. *Manipulación informática*

Se trata de acciones del ciberdelincuente no autorizadas de modificación en el sistema de información utilizado; corresponden a la conducta de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones o que no se lleven a cabo las incorrectas[115].

---

[113] Hidalgo Banilla, Antonio, *op. cit.,* p. 184.
[114] *Idem.*
[115] Paloma Parra, Luis Orlando, *op. cit.,* p. 58.

Con esta conducta se constituye en su completa expresión lo tipificado como delito informático por el Código penal Federal en sus artículos 211 bis 1 al 211 bis 7, pues el sujeto activo al manipular el programa modifica, altera u oculta la información contenida en los sistemas o equipos informáticos.

Es muy común y a menudo pasa inadvertido debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Un método común utilizado por las personas que tienen conocimientos especializados en la programación informática es el denominado Caballo de Troya[116].

Esta modalidad en la que se ejecuta el delito informático solo puede ser constituida por una persona que tenga las habilidades en el campo de la informática, que a la vez se va a basar en ejecutar la conducta del Caballo de Troya para manipular el sistema.

9. *Piratería informática*

Un pirata informático es alguien que utiliza una computadora y red o conexión a Internet para introducirse dentro de otra computadora o sistema para cometer un acto ilegal, esto puede significar simplemente rebasar los límites o actos que corrompan, destruyan o modifiquen datos[117].

Aparte de destruir o modificar los datos contenidos en un sistema o equipo informático, esta conducta va con el propósito de la reproducción no autorizada de la información que se obtenga, lo que conlleva a la ejecución de una pluralidad de conductas delictivas al atentarse en contra de los derechos de autor.

La piratería está asociada con los delitos en contra de la propiedad intelectual, y es la Internet y los diversos sistemas de cómputo, una herramienta para atentar en contra de los derechos de autor (*copy right*) de los inventos, al de las marcas y las patentes[118]

[116] Romero López, Lucero (coord.), *op. cit.,* p. 188.
[117] Norton, Peter, *op. cit.,* p. 549.
[118] López Calvo, Pedro*, op. cit.,* p. 438.

Por lo tanto, la piratería informática es un acto ilícito que aparte de estar tipificada por los artículos 211 bis 1 al 211 bis 7 del Código Penal Federal que se encargan de proteger a la información contenida en sistemas y equipos informáticos, también regulada por la Ley Federal de Derechos de Autor.

Dicha ley establece en artículos 13 fracción IX, y del 101 al 114 la protección a los programas de computación y las bases de datos pertenecientes a su autor, en el sentido, de que este mismo goce de sus privilegios exclusivos de carácter personal y patrimonial, con la facultad de autorizar o prohibir su uso a terceros.

De la misma manera el Código Penal Federal en los artículos 424 al 429 son relativos a los delitos en materia de derecho de autor, que establecen los supuestos ilícitos para quien produzca, reproduzca, o venda los contenidos protegidos por la Ley Federal de Derechos de Autor.

Téllez Valdés afirma que a menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder en aquellos sistemas en los que los usuarios pueden emplear contraseñas comunes o de mantenimiento que están en el sistema[119].

La forma en la que operan los piratas informáticos es en acceder a los sistemas o equipos informáticos haciéndose pasar por el autor de mismo, con el objeto de copiar la información contenida en ellos y reproducirla para lucrar esta con para obtener ganancias económicas.

10. *Hacking*

De Miguel Molina y Oltra Gutiérrez definen al *hacking* como las técnicas para acceder a un sistema informático sin autorización. Existente autorización cuando se dispone de control de acceso mediante el uso de identificadores de usuario o *passwords*[120].

[119] Téllez Valdez, Julio, *op. cit.,* p. 195.

[120] Miguel Molina De, María del Rosario y Oltra Gutiérrez, Juan Vicente, *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas,* España, Editorial de la UPV, 2007, p. 119.

Esta conducta ilícita la pueden realizar solamente las personas que tengan los conocimientos informáticos suficientes para romper las contraseñas de los equipos, sistemas informáticos o redes; es decir, la conducta de *hacking* es el acceso sin autorización a un sistema informático con el objeto de atentar en contra de la información o bien, solamente para conocerla.

Hocsman comenta al autor Líbano, quien dice que el *hacking* puede ser directo o indirecto:

El *hacking* directo es un delito informático que consiste en acceder de manera indebida, sin autorización, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de códigos de acceso o *passwords,* no causando daños inmediatos y tangibles a la víctima o bien por la mera voluntad del autor de curiosear o de divertirse[121].

Con este tipo de *hacking,* el hacker, lo único que intenta realizar es probar o demostrar sus habilidades informáticas, por lo que a la vez se constituye como un delito porque se está accediendo sin autorización a sistema o equipo informático, que, aunque no daña o modifica la información contenida en el sistema si comete la conducta ilícita de conocerla.

El *hacking* indirecto es aquel que se utiliza como medio para la comisión de otros delitos como el fraude, sabotaje o piratería informática. El ánimo del delincuente está determinado por su intención de dañar, de defraudar, dándose la hipótesis del concurso ideal o formal de delitos[122].

Es decir en el *hacking* indirecto conforma un delito informático en el que intervienen una conducta, lo que viene siendo el acceso no autorizado a un sistema o equipo informático, con la realización de dicha conducta se ejecutan una serie de delitos (fraude, sabotaje, piratería informática o manipulación de programas, robo o apoderamiento de información o la ejecución de bombas cronologías, caballos de

[121] Hocsman, Heriberto Simón, *Negocios en Internet,* Colombia, Editorial Astreas, 2013, p.253.
[122] *Idem.*

Troya o gusanos informáticos), es decir una pluralidad de delitos, hay unidad de conducta y pluralidad de resultados.

11. *Cracking*

Hocsman señala que la diferencia entre *cracking* y *hacking* indirecto es que, en el primero, además de configurarse un acceso ilegitimo al sistema de información, lo daña o se altera con voluntad dolosa de provocar daño, sin que se produzca un concurso ideal de figuras[123].

El autor que ejecuta esta modalidad de *cracking,* tiene toda la intención y voluntad de comisionar la conducta ilícita, es decir, es un sujeto hábil en los sistemas informáticos que actúa con el dolo de modificar, destruir, provocar perdida de la información, conocerla o copiarla

Con el *cracking* sólo se constituye una conducta ilícita, esta puede ser cualquier conducta, con la que se pueden ejecutar las diferentes modalidades de delitos informáticos, es decir, que la intromisión al sistema o equipo informático sea voluntaria y dolosa se ejecute un virus informático, una bomba lógica o por una manipulación de programas.

## VI. CONDUCTAS INFORMÁTICAS NO TIPIFICADAS QUE AFECTAN BIENES JURÍDICOS FUNDAMENTALES

Hoy en día todos los medios informáticos incluidos en ellos la Internet, por la vulnerabilidad informática ofrecen facilidades para que se comisionen una serie de conductas delictivas que lesionan diferentes bienes jurídicos de las personas, más allá de los que ya se encuentran protegidos por la ley.

Estos medios informáticos propagados por el territorio mexicano son manejados por los ciberdelincuentes como las herramientas fundamentales en las que llevan a cabo el delito, utilizándolas como el medio para realizar ilícito y llegar al fin cometido.

[123] *Idem.*

No solo la informática en sí misma está siendo amenazada, sino, también una serie de bienes y derechos que las leyes tutelan se ven vulnerados por criminales que utilizan las computadoras y al Internet como instrumentos para cometer sus ilícitos[124].

Con el desarrollo y la proliferación masiva de las redes sociales en las últimas dos décadas han aparecido otras conductas delictivas informáticas, las que aún no se encuentran tipificado su contenido en el Código Penal Federal, el cual solo protege a la información electrónica.

> En el ámbito penal, se abre el debate sobre la naturaleza de los tipos penales a través de los que se introducen estos abusos de los sistemas de información, sobre su objeto de protección general y sobre la necesidad, o no, de regular de alguna forma específica aquellos delitos en los que se participan con mayor o menor intensidad los sistemas informáticos[125].

La creación o renovación de los tipos penales en los que intervienen las nuevas tecnologías, es una problemática legislativa que se debe de atender de forma adecuada e inmediata, pues están en riesgo bienes jurídicos fundamentales de las personas.

Para estudiar estas conductas delictivas que se desprenden de las tecnologías informáticas, las vamos a clasificar en conforme al bien jurídico que afectan, entre ellos está el bien jurídico del patrimonio y el bien jurídico relacionado con la paz y la seguridad de las personas

1. *El bien jurídico del patrimonio afectado por las conductas ilícitas informáticas*

El patrimonio es uno de los principales bienes jurídicos fundamentales de las personas, que se ha visto afectado o lesionado por las diferentes conductas

[124] Villa, Escobosa, Jaime, "Los delitos informáticos", *op. cit.* p. 239.

[125] González Hurtado, Jorge Alexandre, "La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española", *Revista Penal México,* México, 2016, Número 9, Septiembre de 2015- enero 2016, p. 60.

delictivas informáticas existentes, de las cuales, el Código Penal Federal en sus tipos penales aun no las regula de la forma adecuada.

De esta manera, Muñoz Conde define al patrimonio como el conjunto de derechos y obligaciones, referibles a cosas u otras entidades, que tienen un valor económico y que deben ser valorables en dinero[126].

Asimismo el patrimonio de las personas es un elemento fundamental para el buen desarrollo del hombre en sociedad, pues lo conforman un conjunto de bienes de carácter pecuniario con los cuales las personas satisfacen sus diferentes necesidades.

En consecuencia, con lo anterior, ante la comisión de alguna de las variadas conductas delictivas que se basan de la informática para lesionar, se generan grandes pérdidas económicas de carácter grave e incluso algunas pueden ser irreparables.

Las conductas delictivas informáticas que afectan el patrimonio, están estrechamente ligadas con los delitos que se comenten en materia financiera, debido a que en la mayoría de los casos el patrimonio de las víctimas que se encuentran resguardado en las instituciones financieras.

En materia financiera se encuentra una incidencia alta de conductas delictivas que afectan en forma importante a los usuarios de servicios financieros y a las instituciones financieras por igual, en el que los delincuentes utilizan los sistemas informáticos y electrónicos para cometer sus ilícitos[127].

Las instituciones financieras también se ven afectadas por las conductas delictivas informáticas, que van encaminadas a afectar el patrimonio de las personas sean físicas o morales con los comúnmente llamados fraudes informáticos que se comenten por los medios informáticos.

---

[126] Muñoz Conde, *Derecho penal parte especial,* 14 a ed., España, Tirant Lo Blanch, 2002, p. 352
[127] Villa, Escobosa, Jaime, "Los delitos informáticos", *op. cit.,* p. 260.

Así pues, Miguel de Molina define al fraude informático como la conducta que consiste en la utilización de programas de ordenadores, en beneficio propio o de un tercero ocasionando un daño patrimonial a una persona[128].

Así mismo el propósito fundamental del fraude informático es atentar gravemente en contra del bien jurídico del patrimonio de las personas, en el cual, el sujeto activo recibe una ganancia, fruto, o utilidad de carácter lucrativa para sí mismo y/o para un tercero.

Por consiguiente Marcos G. Salt refiere que, al fraude común, el fraude informático consiste en la manipulación ilícita a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas[129].

El delito de fraude común se encuentra regulado por el C.P.F., por el título vigésimo segundo en el capítulo denominado delitos contra las personas en su patrimonio, procedente al artículo 386, en el cual, el tipo penal establece que se comete el delito de fraude, el que engañando a uno o aprovechándose del error en el que éste se halla se hace ilícitamente de una cosa o alcanza un lucro indebido.

En un análisis literal por el artículo 386 del Código Penal Federal, podemos notar que se establecen una serie de conductas tipificadas como fraude, en ellas, no se encuentra la regulación jurídica que éste tipo penal sea cometido por medios informáticos, por lo que existe una omisión legislativa hacia este tipo de conducta.

Algunos de los riesgos actuales por el uso de medios electrónicos e informáticos en actividades financieras son: robo de identidad, robo de claves de acceso y número de identificación personal, y la realización de operaciones financieras sin autorización de las personas legitimadas para ello[130].

Del fraude informático se desprenden diversas conductas, una de ellas es la usurpación de identidad por medios informáticos, esta conducta en la doctrina es

---

[128] Miguel Molina De, María del Rosario y Oltra Gutiérrez, Juan Vicente, *op. cit.,* p. 110.
[129] G. Salt, Marcos, "Los delitos informáticos de carácter económico", *op. cit.,* p. 236.
[130] *Idem.*

mayormente denominada como robo de identidad, el cual es bastante grave, se atenta en contra de la identidad de las personas con el objeto de usurparla y de afectar su patrimonio o en su propia persona.

Así pues, López Calvo nos dice que el robo de identidad consiste en que la información personal de un individuo, tal como la información identificable, financiera o médica ha sido obtenida y utilizada sin su consentimiento y con el propósito de cometer una actividad ilícita fraudulenta[131].

Esta conducta que se ejecuta por medio de sistemas informáticos consiste en que el ciberdelincuente se encarga de sabotear los datos personales de naturaleza bancaria, de su víctima para hacerse pasar por ella accediendo a sus cuentas y robarle cantidades de dinero o bien obtener créditos.

Los delincuentes informáticos que ejecutan la usurpación de identidad por medios informáticos han hecho de este un delito muy complejo, del cual se desprenden otras series de variantes especificadas en la doctrina como *phising,* que va también con el propósito de lesionar el bien jurídico del patrimonio.

> El *phishing* se define como actividad delictiva que supone el envío indiscriminado de correos electrónicos (a modo de anzuelo), con la finalidad de que alguna de las persona que los reciba "pique" y acceda a una página web que se ha imitado para hacer creer al visitante que se encuentra en la página original normalmente de bancos conocidos, en lugar de una copiada, y una vez en dicha página falsa, acabe de tragarse el anzuelo, introduciendo los datos de acceso al banco[132].

La finalidad de la modalidad del *phishig* es engañar a la persona por medio de sus tres pasos para que esta revele sus datos personales y se le robe su identidad, sin duda, esta modalidad solo la puede ejecutar una persona que tenga la pericia suficiente en los medios informáticos.

---

[131] López Calvo, Pedro*, op. cit.,* p. 441.
[132] Sanchis Crespo, Carolina (coord.), *Fraude electrónico: entidades financieras y usuarios de banca,* Editorial Aranzadi, España, 2011, p. 105.

En suma de lo anteriormente señalado, podemos inferir que el fraude informático es una conducta con gran lesividad para el patrimonio de las personas, que debe de ser incorporado en el C.P.F. en sus tipos penales, así como también se deben de prever la variante de *phishing.*

2. *El bien jurídico de la paz y la seguridad de las personas afectado por las conductas delictivas informáticas*

Terminando con las conductas que lesionan el bien jurídico del patrimonio, ahora procederemos a analizar aquellas conductas delictivas que parten de los sistemas informáticos para dañar otro bien jurídico fundamental del ser humano como lo es paz y la seguridad de las personas.

En estos últimos años con la masiva expansión de la Internet, la proliferación de los dispositivos informáticos y con la popularidad de las redes sociales, han dado lugar que aparezcan una serie de conductas que afectan a la paz y la seguridad de las personas que utilizan estos medios electrónicos. Este bien jurídico se ve afectado no necesariamente por una persona que sea especialista en los sistemas informáticos, sino quienes ejecutan estas conductas son personas comunes que tienen en su posesión un medio informático y quieren lastimar a otras.

Estos bienes jurídicos son tutelados por el derecho penal, sus tipos penales se encuentran rezagados, debido a que aún no se han adecuado al nuevo contexto social en la forma que se necesita para una protección integral a este bien jurídico. El fenómeno de conductas ilícitas se compone por comportamientos que se conocen como *ciberbullyng* o ciberacoso, en las cuales las principales víctimas son menores de edad.

El *ciberbullyng* o ciberacoso consiste cuando un niño, adolescente o preadolescente, es atormentado, amenazado, acosado, humillado y avergonzado por otra persona desde Internet, mediante medios interactivos, tecnologías digitales y teléfonos móviles[133].

[133] García González, Javier (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant Lo Blanch, España, 2010, p. 56.

Actualmente la conducta de *ciberbullyng* o ciberacoso es muy frecuente principalmente en las redes sociales, de las que se tiene que tener sumamente cuidado porque en un buen número de casos causan trastornos psicológicos en los menores.

Los menores habitan en el Internet. Bautizados como nativos digitales, ellos son los usuarios de *Smartphones* y *tablets* que más supervisión y educación digital requieren. Privarles de un conocimiento detallado y conciso de este mundo les puede convertir en víctimas o en autores de un delito[134].

Conforme a lo anterior, los padres de los menores de edad y los mismos menores usuarios de las tecnologías informáticas y de la Internet deben de tener mucho cuidado de su actuar en la Red, ya que estos se pueden ser las víctimas o bien, sin darse cuenta en agresores. Un sujeto sin darse cuenta se puede convertir en un agresor debido a que el ciberacoso es una conducta que empieza entre los sujetos de forma casual que posteriormente se va agravando llegando hasta humillar, amenazar, atormentar, avergonzar a la otra persona.

El C.P.F en el titulo decimoctavo denominado delitos contra la paz y la seguridad de las personas, en el artículo 282 regula las amenazas en contra de las personas, pero no tipifica que estas sean por medios informáticos, ni tampoco regula las conductas de humillar, amenazar, atormentar, avergonzar.

Por ende, debido a la gravedad de las conductas expuestas, es que el legislador debe de tipificar estas conductas, adecuando los tipos penales a los contextos sociales existentes de forma inmediata con el objetivo de frenar la comisión de este tipo de ilícitos.

[134] Cervantes, Pere y Tauste Oliver, *Internet negro,* Ediciones Culturales Paidós, México, 2016, p. 71.

# CAPÍTULO TERCERO

# LOS DELITOS INFORMÁTICOS EN EL DERECHO COMPARADO

## I. PANORAMA LEGISLATIVA INTERNACIONAL ACTUAL

### 1. *Cooperación internacional legislativa en los delitos informáticos*

En los delitos informáticos la cooperación internacional es un factor muy importante para la prevención de los mismos, por ello, éste apartado atiende por qué obedece a la necesidad de la uniformidad y la armonía legislativa entre países, así como también la manera en la que estos mismos han contribuido al legislar estos actos como tipos penales.

Asimismo, Villa Escobosa refiere que en el contexto internacional, algunos países cuentan con una legislación que contempla específicamente los llamados delitos informáticos, entre los que se encuentran Alemania, Austria, Chile, España, Estados Unidos, Francia, Gran Bretaña, Holanda, Italia, y Venezuela[135].

Estos países que ya han tipificado los delitos informáticos forman parte de la cooperación internacional, en ese sentido, que se contemplen estas figuras en sus leyes no es suficiente, pues lo que se requiere es que todas ellas cuenten con una uniformidad y armonía legislativa.

Para ello, se requiere del Derecho Penal Internacional, en el plano que este mismo, se ocupe de dirigir las normas comprendidas por el Derecho Internacional estableciendo la responsabilidad penal a los autores y/o participes de estos delitos, además también de orientar su prevención.

Hernández García Joel, expresa que esta es una rama del Derecho Internacional que ha cobrado una gran vigencia desde el momento en que la

[135] Villa Escobosa, Jaime, *"Los delitos informáticos",* en Durán Díaz, Oscar Jorge (coord.), *Derecho y medios electrónicos, temas selectos,* México, Porrúa, 2012, p. 252.

comunidad internacional decidió cooperar para combatir distintas conductas ilícitas dentro de las cuales debemos incluir desde luego a los delitos cibernéticos[136].

Así pues, los delitos informáticos son considerados importantes para el Derecho Penal Internacional, porque, estos mismos adquieren la característica de ser delitos trasnacionales, que afectan en diversas direcciones territoriales es decir, con ayuda de la Internet, traspasan las barreras territoriales de un Estado a otro.

Hoy en día es muy común que un delito se planee dentro del territorio de un Estado, se desarrolle en el territorio de otro Estado, tenga consecuencias en el territorio de un tercer Estado, sus autores sean de distinta nacionalidad, las víctimas del delito tengan a su vez otra nacionalidad[137].

En efecto, debido a la globalización de los sistemas informáticos y de la Internet, los delitos informáticos se inmiscuyen en gran parte del mundo, lo que provoca que se afecte la esfera jurídica de cada Estado en donde se actué, es por ello que se requiere de una cooperación internacional de tutela efectiva.

Cada Estado en donde se realice la comisión de un delito informático, ya sea en relación a su territorio o por nacionalidades de sus autores, debe de tener una legislación que contemple la conducta ilícita, pero más que nada, dicha legislación tiene que ser acorde a la otra, estas mismas deben de ser similares respecto a la descripción del tipo penal, así como en los diversos supuestos de hecho que lo componen, el bien jurídico protegido y la consecuencia jurídica que se pretende aplicar.

La problemática que se observa a nivel internacional tiene varios frentes y vertientes; falta de definición en las diversas leyes de lo que es la conducta delictiva;

---

[136] Hernández García, Joel, "Cómo examinar el problema del crimen cibernético a nivel internacional" en Comisión Nacional de los Derechos Humanos, *Avances tecnológicos de los Derechos Humanos, fascículo 4,* México, Comisión Nacional de los Derechos Humanos, 2004, p. 61.
[137] *Ibidem,* p. 62.

falta de uniformidad entre los ordenamientos jurídicos de los distintos países al referirse a estas conductas; deficiente cooperación internacional entre países[138].

En consecuencia, lo que se pretende para mejorar la cooperación internacional entre países, es que estos mismos empiecen a participar internacionalmente, legislando de forma clara y precisa las conductas de la ciberdelincuencia para así cubrir los vacíos legislativos existentes, así como también las omisiones legislativas.

Es muy importante precisar acorde al principio de legalidad, que los tipos penales deben de estar bien asentados siendo estos claros en el injusto penal, el bien jurídico que se protege reconocido por el Estado, los elementos objetivos y subjetivos, los sujetos del delito y el objeto material del delito

Consideramos que una viable forma de mejorar la cooperación internacional entre los países, es que estos mismos ratifiquen instrumentos internacionales tales como pactos, acuerdos, tratados internacionales y también que muestren su participación en convenciones internacionales en materia de delitos informáticos o ciberdelincuencia.

Por ello, la ONU promueve que sus Países Miembros a regular estas conductas en sus legislaciones, tal fue el caso como en año de 1999 lo hizo con México (véase las páginas 63 a la 66 del segundo capítulo de la presente investigación) para que contribuyera con la cooperación internacional.

Esto trajo consigo que México se pusiera a la par con países como Alemania, Austria, Francia, España y Estados Unidos, al incorporar en el Código Penal Federal los artículos 211 bis 1 al 211 bis 7 el 17 de mayo 1999 debido a que México no contaba estas figuras en su C.P.F.

La aproximación del derecho positivo en materia de delincuencia informática contribuirá, a que las legislaciones sean lo suficientemente completas para que

[138] Villa Escobosa, Jaime, *"Los delitos informáticos",* en Durán Díaz, Oscar Jorge (coord.), *op. cit.,* p. 241.

todas las formas de ataques contra los sistemas de información puedan ser objeto de investigaciones, mediante técnicas y métodos disponibles en el derecho penal[139].

Debido a lo anterior, es que se solicita a los países a regular estas figuras en sus legislaciones, a causa de hacer efectivo el principio penal *nullum crimen, nulla poena sine previa lege,* que establece, no hay delito, no hay pena sin previa ley, y así evitar atipicidades y con ello la impunibilidad de los responsables.

> Por su parte, Cruz de Pablo afirma que, el Manual de las Naciones Unidas para la Prevención y Control de los Delitos Informáticos, señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto, los delitos informáticos constituyen una nueva forma de crimen trasnacional y su combate requiere una eficaz cooperación internacional concentrada[140].

Asimismo, la ONU como organismo internacional, con atribuciones de brindar recomendaciones para regular conductas, y encargada de proteger el derecho internacional de los Estados Miembros, tiene la facultad de interferir para mantener la seguridad internacional, cuando un delito de naturaleza trasnacional afecta bienes jurídicos fundamentales, como es el caso de los delitos informáticos.

La ONU lleva acabo la función de realizar consecutivamente congresos, convenios, acuerdos y pactos con sus Estados Miembros para que estos cooperen internacionalmente con el propósito de lograr una uniformidad legislativa, todo con el fin de fortalecer a la comunidad internacional en contra del cibercrimen.

La uniformidad en las legislaciones mejorará esta cooperación y garantizará que se cumpla con la exigencia de la doble incriminación (según la cual una actividad debe constituir un delito en los dos países en cuestión, para que estos colaboren a nivel judicial en el marco de la investigación penal)[141].

---

[139] Flores Salgado, Lucerito, *Derecho informático,* México, Editorial Patria, 2009, p. 134.
[140] Cruz de Pablo, José Antonio, *Derecho penal y nuevas tecnologías. Aspectos sustantivos,* España, Grupo Difusión jurídica y temas de actualidad, 2006, p. 174.
[141] Hidalgo Banilla, Antonio, *Derecho informático,* México, Flores editor y distribuidor, 2013, pp. 189 y 190.

Al tipificarse estas conductas como delito en diversos países, se abre el camino de criminalizar al responsable del delito dentro de su territorio, y con esto, también se coopera internacionalmente con otros países, al establecerse las disposiciones pertinentes a la figura de la extradición, por ello, es muy importante la uniformidad y armonía legislativa entre países.

Ahora bien, comenzaremos a analizar de qué manera algunos países han contribuido internacionalmente legislando estas figuras lesivas en sus códigos penales y leyes, con el objeto de interpretar sí sus tipos penales corresponden a fortalecer una uniformidad y armonía legislativa hacia los demás países.

> Por ello, Gustavo Aboso nos dice: la legislación sobre delitos informáticos en Austria se remonta hasta 1978, fecha en la cual se sanciona la primera ley de protección a la información. Esta ley ya preveía en su artículo 48 el tipo penal de violación de secreto, y en el artículo 49 el ingreso no autorizado a una red de información[142].

De este modo, Austria fue uno de los primeros países en regular este delito en sus leyes, con la idea de tutelar la información contenida en equipos y sistemas informáticos, ante ataques no autorizados que puedan ser lesivos a las violaciones de secretos que en ella se contenga.

En complementación Montoya piña refiere: en el Reino Unido básicamente son dos las leyes relativas a la utilización de equipo superior que han sido aprobados por el Gobierno británico, estas leyes son la ley de protección de datos de 1984 y la ley de uso indebido de un equipo de 1990[143].

Asimismo, el Reino Unido posee una de las regulaciones más amplias respecto a este delito, al regular sus modalidades en dos leyes diferentes, por un

---

[142] Aboso, Gustavo Eduardo y Zapata, María Florencia, *Cibercriminalidad y derecho penal*, Argentina, Editorial B de F, 2006, p. 194.

[143] Montoya Piña, Javier Omar, *Delitos federales cometidos a través de medios informáticos,* México, Flores editor, 2015, p. 31

lado se tutelan los datos informáticos, y por otro, se tutela el uso ilícito de equipos y sistemas informáticos ante ataques de intromisiones de carácter ilícito.

Por su parte, en Portugal los delitos informáticos se encuentran regulados por la ley n° 109/91. Esta ley regula el delito de falsedad informática (art. 4°); el daño a programas informáticos (art. 5°); el sabotaje informático (art. 6°); acceso de forma ilegítima a un sistema (art. 7°); la interceptación ilegitima (art. 8), entre otras[144].

La regulación jurídica de Portugal respecto hacia estos delitos, es muy amplia, debido a que dedica una ley exclusiva para regular estas conductas delictivas, en esta misma se tutela no solo a la información contenida en sistemas y equipos informáticos, sino también a los mismos programas y sistemas informáticos ante daños que pudieran ocurrir en su funcionamiento.

Entre tanto, hasta aquí hemos analizado en *grosso modo* la forma en la que Austria, Reino Unido y Portugal, han cooperado internacionalmente al regular este tipo de delito en su ordenamiento jurídico; pero ¿cómo se regula a estas conductas ilícitas en Latinoamérica?, pues bien ahora lo analizaremos.

Para ello, Flores Salgado refiere: Chile fue el primer país latinoamericano en sancionar una ley contra los delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los delitos de destrucción de datos, conducta maliciosa tendiente a la destrucción, daño, alteración de datos, entre otras más[145].

En Latinoamérica, Chile representa ser un país comprometido con la cooperación internacional al regular estas conductas delictivas en su territorio por una ley que contempla, las diferentes modalidades con las que se puede atentar en contra de la información contenida en sistemas y equipos informáticos.

Asimismo también en Latinoamérica, Perú en su Código Penal contempla, en su Capitulo X, bajo la rúbrica “Delitos informáticos”, el delito de ingreso no

[144] *Ibídem,* pp. 195 y 196.
[145] Flores Salgado, Lucerito, *op. cit.,* p. 138.

autorizado a una base de datos (art. 207.a) y el de alteración o destrucción de datos (art. 2017.b)[146].

Dicho país reglamenta estas figuras con el tipo penal de delitos informáticos, lo que consideramos que el tipo penal no corresponde a ser uniforme con los demás países tanto del continente Europeo como de Latinoamérica porque lo regula con el tipo penal de "Delitos informáticos", lo que conlleva que no haya una uniformidad y armonía legislativa.

Después, en Venezuela en el 2001 se promulgo la Ley Especial contra los delitos informáticos por la Asamblea Nacional de la República Bolivariana de Venezuela. Argumentados en los capítulos: De los Delitos Contra los Sistemas que Utilizan Tecnologías de la información y De los Delitos Contra la Privacidad[147].

Por su parte, el país venezolano también se une a la cooperación internacional al incorporar en su ordenamiento jurídico una ley especial, que sus capítulos corresponden a ser uniformes con los países anteriormente analizados, y además en esta misma incorpora las TIC, lo que conlleva a que esta ley plantea aspectos actualizados a las nuevas tecnologías.

Asimismo, Nava Garcés apunta que resulta indispensable, establecer la cooperación internacional como uno de los puntos de solución, al problema de la cibercriminalidad más aun tomando en cuenta que, el que no participa conjuntamente significa un riesgo[148].

Conforme a lo expuesto en líneas anteriores, podemos apreciar la importancia que significa que los países conjuntamente cooperen internacionalmente en contra del cibercrimen, más aun, cuando sabemos que este es un delito de naturaleza trasnacional.

---

[146] Aboso, Gustavo Eduardo y Zapata, María Florencia, *op. cit.,* p. 200.
[147] Montoya Piña, Javier Omar, *op. cit.,* p. 34.
[148] Nava Garcés, Alberto Enrique, *Análisis de los delitos informáticos,* 2a. ed., México, Porrúa, 2007, p. 140.

Sabemos que no todos los países del mundo se han unido a la cooperación internacional en contra de conductas clasificadas como delito, lo que conlleva a una des variación que desarmoniza el derecho penal en el contexto internacional.

Afganistán, Albania, Andorra, Bahamas, Barbados, Belice, Camboya, Fiji, Georgia, Haití, Islandia, Isla Marshall, Israel, Letonia, Malawi, Maldivas, Mónaco, Mongolia, Santo Lucia, Serbia, Santo Tomé y Príncipe, Sudán del sur, Tonga, Tuvalu, Uzbekistán, entre otros[149].

Estos países, por mencionar unos cuantos, nunca han elegido Miembros para el Consejo de Seguridad de las Naciones Unidas desde 1946, como podemos ver la mayoría pertenecen al derecho religioso, ¿será porque la cultura jurídica de este tipo de familia jurídica no está de acuerdo con el derecho codificado o con el derecho jurisprudencial?, ¿o acaso será por qué su norma principal es el Corán?

A lo anterior se le ha denominado como paraísos para los delitos informáticos, es decir, territorios desde los cuales se podrían ejecutar algunas de tales conductas sin temor a recibir sanción penal, puesto que los ordenamientos penales vigentes de dichos lugares no las consideran como delictivas[150].

No obstante, todos estos mismos deben de seguir el camino de buscar la seguridad de sus naciones, y la mejor manera es prestándose a los principios que ofrece la cooperación internacional y demás organismos internacionales, porque, de no ser así se pone en riesgo la afectación de bienes jurídicos de la comunidad internacional.

2. *Los delitos informáticos en la legislación de Alemania comparada a la legislación mexicana*

Para comenzar con este subtema procederemos a realizar un estudio de comparación entre la legislación de Alemania y el Código Penal Federal de México,

[149] https://www.un.org/securitycouncil/es/content/countries-never-elected-members-security-council
[150] Galán Muñoz, Alfonso, *El fraude y la estafa mediante sistemas informáticos análisis del artículo 248.2 del C.P.,* España, Tirant lo Blanch, 2005, p. 42.

en torno a la institución jurídica del delito de Acceso ilícito a sistemas y equipos de informática, denominado también por la doctrina jurídica como delito informático.

Asimismo apreciamos que en Alemania se tiene muy clarificada la legislación acerca de las conductas ilícitas informáticas, por ello procederemos a analizar el Código Penal Alemán y compararlo con el C.P.F. para encontrar similitudes y diferencias en ambas legislaciones.

De este modo, Hocsman refiere que en Alemania la ley contra la criminalidad económica de 1986 fue una de las pioneras en penalizar ciertas conductas que tipifican delitos informáticos. Entre éstos se encuentran: el espionaje de datos, el fraude informático, delito de daño, y el sabotaje informático[151].

Mientras tanto, el Código Penal Federal reguló dichas conductas ilícitas hasta el año de 1999, por lo que podemos ver, que nos tardamos quince años en contemplar estas figuras, lo que nos lleva a pensar que en México padece de rezago en materia de legislación.

Como señala Nava Garcés, en el Código Penal de Alemania observamos los delitos contra los datos o las informaciones. Las formas típicas del derecho alemán son: el espionaje informático (artículo 202 a); estafa informática (artículo 263 a); destrucción de datos (artículo 303 a) y sabotaje informático (artículo 303)[152].

Por ende, a *prima facie* podemos notar que el Código Penal de Alemania tiene una técnica legislativa distinta al C.P.F., pues en este se sanciona a las conductas típicas de la informática en tres títulos diferentes, variando el bien jurídico a proteger y el tipo penal que las conforma.

Por un lado, se encuentran en el título Violación de la vida personal y área secreta, los tipos penales de espionaje de datos, interceptación de datos, y preparación para la interceptación de datos, con el objetivo de resguardar el bien jurídico de la intimidad personal en su carácter de datos informáticos.

---

[151] Hocsman, Heriberto Simón, *op. cit.,* pp. 268 y 269.
[152] Nava Garcés, Alberto Enrique, Análisis de los…, *cit.,* pp. 108 y 109

El segundo título es el correspondiente a fraude, mismo que lo regula con el mismo tipo penal, pero, haciendo énfasis a fraude informático, para así proteger a los datos informáticos de carácter financiero ante conductas ilícitas que los puedan alterar o sustraer del sistema informático.

Y por último, en el título de daños a la propiedad con los tipos penales de modificación de datos y sabotaje informático, resguardando el bien jurídico de la información contenida en un sistema o equipo informático ante ataques de eliminar o interceptar dicha información.

Así pues, Paloma Parra refiere que en la legislación alemana existen diversos preceptos penales, como el intrusismo sin autorización o la sola sagacidad no autorizada en sistemas ajenos de computadoras, asimismo también se sanciona el uso no autorizado de aparatos de procesos de datos[153].

Las dichas conductas anteriores, se encuentran reguladas por el artículo 202 a del Código Penal de Alemania, al mismo le corresponde a la figura de espionaje de datos como conducta típica, con una penalidad de hasta tres años de prisión, a quien sin autorización acceda superando la seguridad de acceso de un sistema informático que contenga datos no destinados para él.

Luego entonces, en el segundo párrafo de este mismo artículo se precisa que por datos se entiende aquellos que son electrónicos, magnéticos, perfectiblemente almacenados o transmitidos, de esta manera, podemos ver que el legislador tuvo la suspicacia de definir qué se entiende por datos para clarificar estos preceptos.

Por el contrario, el Código Penal Federal de México regula en los artículos 211 bis 1 al 211 bis 7 el acceso ilegitimo con o sin autorización a un sistema o equipo informático, pero con la modalidad que ese acceso provoque una modificación, destrucción o pérdida de información.

[153] Paloma Parra, Luis Orlando, *Delitos informáticos (en el ciberespacio),* Colombia, Ediciones jurídicas Andrés Morales, 2012 p. 214.

En cambio, como pudimos observar en la legislación de Alemania se penaliza a quien acceda ilícitamente a datos informáticos, sin que los modifique, destruya o les provoque alguna pérdida, por lo que a México sólo se contemplan las conductas de conocer o copiar información, pero se deja sin penalidad a quienes no las modifique, destruya o provoque perdida, de esta manera apreciamos que existe una omisión legislativa hacia este precepto legal.

Por otro lado, el artículo 202 b del Código Penal de Alemania es referente a la figura de interceptación de datos que nos dice: a quien no estando autorizado a medios técnicos no destinados para él, a una trasmisión de datos no pública o de la radiación electromagnética, o a un sistema de procesamiento, será encarcelado hasta por dos años o con una multa, si el delito no está regulado en otras disposiciones con penas más severas.

Luego entonces, el artículo 202 c del Código Penal de Alemania muestra como ilícito el acto de preparación para la interceptación de datos: cualquier persona que prepare una ofensa criminal de los artículos 202 a y 202 b, por medio de contraseñas u otros códigos de seguridad que permitan el acceso a datos, o a programas informáticos, con el propósito de vender o distribuir dichos datos a otros se le castigará con una pena de prisión de hasta un año o una multa.

En ese sentido, el C.P.F de México carece también de estas dos disposiciones, plasmadas en los artículos anteriores referentes a la interceptación de datos y la preparación de la interceptación de datos, mismas que afecta a la información que se pueda contener en un sistema o equipo informático.

De este modo, podemos referir que la interceptación de datos es un acto que afecta sustancialmente a la información contenida en equipos y en sistemas informáticos, y en México no se encuentra regulado este acto, por lo que vemos que en nuestro país esta modalidad pasa por alto, y ante lo precisa que es la ley para sancionar a una persona que intercepte datos electrónicos no sería merecedor de pena, por no estar regulada esta disposición en una ley aplicable para el caso.

Así, el artículo 263a del Código Penal de Alemania regula el delito de fraude informático, a cualquier persona que tenga la intención por sí mismo o por un tercero una ventaja financiera ilegal por diseñar ilícitamente un programa mediante usos de datos incorrectos o incompletos o a través del uso no autorizado de datos o influenciado en el proceso, se le encarcelará con hasta cinco años de prisión.

El C.P.F tampoco regula la modalidad del fraude informático anteriormente descrita por el numeral 263a del Código Penal de Alemania, como ya referimos en el capítulo anterior de este trabajo de investigación (visible en las páginas 81 a la 86), y apreciamos que otros países como Alemania desde 1986 ya regulan este ilícito en su Código Penal.

En cambio, en la vigésima séptima sección del Código Penal de Alemania se regula el tipo penal de daños, por lo que el artículo 303a corresponde a la modificación de datos, que nos dice: a cualquier persona que elimine, suprima, inutilice o cambie datos de manera ilegal se le castigará hasta con dos años de prisión o con una multa, el intento es punible.

En este mismo sentido al párrafo anterior, podemos apreciar que el C.P.F en los artículos 211 bis 1 al 211 bis 5 se equipara a esta disposición, al tipificarse la modificación de datos, pero con las conductas de destruir, o provocar perdida, asimismo apreciamos que en Alemania la figura de tentativa es punible.

De la misma manera, el artículo 303b del Código Penal de Alemania regula el sabotaje informático, a cualquier persona que interfiera seriamente con un procesamiento de datos que es esencial para otro, con la intención de agregar, ingresar, transmitir, dañar, eliminar datos de un sistema de procesamiento, será castigado con una pena de prisión de tres años o una multa.

Así pues, a este mismo artículo se le agrega una agravante para proteger los datos informáticos pertenecientes empresas extranjeras o para las autoridades, dicho de esta manera, la pena se agrava hasta con cinco años de prisión, y si es un caso particularmente grave, la pena puede oscilar hasta los diez años de prisión.

Igualmente, el Código Penal Federal de México también regula la disposición del sabotaje informático en los artículos 211 bis 1 al 211 bis 7, solo que las punibilidades son más bajas al ser la mínima de seis meses y la máxima de ocho años de prisión.

Después de analizar los artículos anteriores correspondientes al Código Penal de Alemania podemos ver que en México se carece de mucha legislación, pertinente en relación a los delitos informáticos, lo que nos lleva a no estar a la par con otros países, por lo tanto no hay armonía ni unificación en los tipos penales.

3. *Los delitos informáticos en la legislación de Francia comparada a la legislación mexicana*

> Francia fue otro de los países en sancionar leyes referentes a la materia mediante la ley 88/19 sobre fraude informático, de 1988. Esta ley tipifica una serie de conductas: el acceso fraudulento a un sistema de elaboración de datos (artículo 462-2), el sabotaje informático (artículo 462-3), la destrucción de datos (462-4) la falsificación de documentos informatizados (artículo 462-5) y el uso de documentos informatizados falsos (artículo 462-6)[154].

Además, Francia también regula estos actos ilícitos en su Código Penal, este mismo, dedica un capítulo exclusivo a las conductas típicas de la informática denominado capitulo III Ataques a los sistemas de procesamiento automatizado de datos, que corresponde a los artículos 323-1, 323-2, 323-3, 323-3-1, 323-4, 323-5, 323-6 y 323-7 de dicho ordenamiento.

Después de este preámbulo de disposiciones legales, procederemos a analizar estos artículos tanto de la ley 88/19 sobre fraude informático como del Código Penal de Francia, para así encontrar similitudes y diferencias entre el Código Penal Federal de México.

[154] Hocsman, Heriberto Simón, *op. cit.,* p. 269.

> Entonces, Flores Salgado apunta que el artículo 462-2 de la ley 88/19 sobre fraude informático sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de este acceso resulta la supresión o modificación de datos contenidos en él o resulta la alteración del funcionamiento del sistema[155].

De igual manera, a la ley 88/19 sobre el fraude informático, el Código Penal de Francia en el artículo 323-1 establece como delito al hecho de acceder fraudulentamente o permanecer en todo o parte de un sistema de procesamiento automatizado de datos con una punibilidad de dos años de prisión y de 30,000 euros de sanción económica.

Este mismo artículo establece varias agravantes: cuando se eliminen o se modifiquen datos en ese acceso ilícito la pena será de tres años de prisión y 45,000 euros y; cuando los datos dañados sean del Estado la pena se aumenta a cinco años de prisión y multa de 75,000 euros; por otra parte el artículo 323-7 establece que el intento a estas conductas típicas serán punibles.

Por ende, este artículo de la ley 88/19 de Francia sobre fraude informático y los mencionados del Código Penal de Francia, se equiparan al artículo 211 bis 1 y bis 2 del C.P.F., al establecerse como conducta típica el acceso ilícito a un sistema suprimiendo, modificando, destruyendo o provocando perdida de información.

Sin embargo lo que carece la normativa del C.P.F es de la falta tipificar el acceso ilícito a un sistema y equipo informático sin que se establezca la modalidad de que con ese acceso se tenga que modificar, destruir o provocar perdida de información, como en Francia si se tipifica con la ley 88/19 sobre fraude informático.

Por otro lado, Nava Garcés dice, el artículo 462-3 de la ley 88/19 sobre fraude informático, sanciona a quien impida o falsee el funcionamiento de un sistema de

[155] Flores Salgado, Lucerito, *op. cit.,* p. 137.

tratamiento automático de datos. El delito de sabotaje informático ya existe, sin embargo, este se ha aplicado más bien tratándose en conductas contra el Estado[156].

Igualmente, el artículo 323-2 del Código Penal de Francia es analógico con el artículo 462-3 de la ley 88/19 sobre fraude informático, al establecer una pena de prisión de cinco años y multa de 75,000 euros, a quien obstruya o distorsione el funcionamiento de un sistema informático y si este sistema es del Estado la penalidad se agrava a siete años de prisión y multa de 100,000 euros.

Luego, Paloma Parra expresa, el artículo 462-4 la ley 88/19 sobre fraude informático dice: a quien con dolo y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento de trasmisión[157].

Así pues, similar al artículo anterior, el Código Penal de Francia también sanciona la destrucción de datos en el artículo 323-3 con una penalidad de cinco años de prisión y 75,000 euros de multa, además de establecer una agravante de siete años de prisión si la destrucción de datos son del Estado.

De igual manera, el artículo 211 bis 2 del C.P.F. sanciona la conducta anteriormente descrita, de uno a cuatro años de prisión y de doscientos a seiscientos días multa, por lo que podemos ver que Francia es más severo en cuestión de las penalidades para este tipo de delito.

Por otra parte, el artículo 462-5 de la ley 88/19 sobre fraude informático, sanciona a quien de cualquier modo falsifique documentos informáticos con la intención de causar perjuicio a otro; y el artículo 462-6 de la misma ley sanciona a quien conscientemente haga uso a los documentos del artículo 462-5.

Luego entonces, en atención a los artículos 462-5 y 462-6 de la ley 88/19 sobre fraude informático podemos ver que el C.P.F carece de estas dos

[156] Nava Garcés, Alberto Enrique, Análisis de los…, *cit.,* p. 121.
[157] Paloma Parra, Luis Orlando, *op. cit.,* p. 225.

disposiciones, pues en sus artículos no se especifica como conducta típica la falsificación de documentos informáticos así como también su utilización.

Conforme al análisis anterior podemos notar que el C.P.F tiene algunas disposiciones similares a la legislación Francesa, sin embargo, son más las diferencias que hemos encontrado tanto en los tipos penales, y sus diversos supuestos, así como también en las penalidades hacia este tipo de delito.

4. *Los delitos informáticos en la legislación de España comparada al Código Penal Federal de México*

Respecto a la regulación de los delitos informáticos, España cuenta con muchas similitudes, como por ejemplo en el tipo penal, denominado Revelación de secretos, pero a la vez, también se presentan notorias diferencias con el Código Penal Federal de México, lo que lleva consigo a estudiar ambos ordenamientos jurídicos para determinar las eficiencias y deficiencias que presentan entre sí, y así poder mejorar la legislación penal mexicana vigente de vacíos legislativos y omisiones legislativas hacia este tipo de delito.

Así pues, Lan Arredondo afirma: España corresponde a la familia neorromanista, la que es la más extendida, ya que el mayor número de sistemas jurídicos nacionales pertenece a esta: casi todos los países de América Latina, de Europa continental, así como un buen número de naciones de Asia y África[158].

De igual manera, México es uno de los países que forma parte de la familia neorromanista, es por ello que hay muchas similitudes y variadas características con la legislación Española, en donde se predomina el culto hacia la ley y por ende también al derecho codificado.

La ley es la fuente principal para la familia neorromanista. La ley conlleva un valor muy parecido para esta familia como lo es la certeza jurídica. Entre los actores

[158] Lan Arredondo, Arturo Jaime, *Sistemas jurídicos,* México, Oxford, 2011, p. 26.

jurídicos que pertenecen a ella es común escuchar que uno de los valores trascendentales para el derecho es la certeza que proviene de la ley[159].

En consecuencia, para darle regulación jurídica en el derecho positivo a los llamados delitos informáticos, estos diversos actos ilícitos que atentan en contra de la información contenida en sistemas y equipos informáticos, han sido incorporadas al Código Penal de España para regular la problemática del ciberdelito.

> Hocsman refiere que en España, el Código penal (ley orgánica de 10/95, aprobada el 23 de noviembre de 1995 y vigente desde el 24 de mayo de 1996) tipificó una serie de delitos que se pueden cometer por medio de Internet. Entre estos destacan: la violación de secretos y apoderamiento, utilización o modificación ilegitima de datos reservados contenidos en medios informáticos; y la destrucción, alteración, inutilización o daño de datos programas o documentos contenidos en redes o soportes informáticos[160].

Las conductas típicas anteriormente señaladas se encuentran reguladas en el Código Penal de España por los artículos 197, 197 bis, 197 ter, 197 quater, 197 quinquies regulando la tutela jurídica de la Revelación de secretos, y por los artículos 264, 264 bis, 264 ter y 264 quater tutelando el bien jurídico del patrimonio.

Como se menciona en la página 65 del segundo capítulo de esta tesis de investigación, México regula estas figuras delictivas después que España, siendo adicionados al C.P.F. en el Titulo noveno denominado Revelación de secretos y acceso ilícito a sistemas y equipos de informática, en los artículos 211 bis 1 al 211 bis 7 el 17 de mayo de 1999, por lo que se puede observar que España tiene una técnica legislativa más rápida para legislar situaciones actuales que México.

> Así pues, Campoli hace mención de: podemos definir que el bien jurídico protegido en este caso sería la integridad de los sistemas informáticos o electrónicos en general, con lo cual se puede afirmar que nos encontramos

[159] *Ibidem,* p. 47
[160] Hocsman, Heriberto Simón, *Negocios en Internet,* Colombia, Editorial Astreas, 2013, p. 273

con sujetos capacitados para producir alguna alteración dañosa en un medio electrónico aunque dentro de un criterio más amplio podemos considerar que lo que se protege es realmente la privacidad o la propiedad informática[161].

De la misma manera, España regula estas figuras de cibercriminalidad en el año de 1996, para no quedarse atrás de otros países del continente Europeo, como Alemania, Austria, Francia, Italia y Holanda quienes son los primeros en tipificar estas conductas antijurídicas en su cuerpo de leyes.

El código penal español sanciona en forma detallada esta categoría delictiva (violación de secretos, espionaje y divulgación) aplicando penas de prisión y multa, agravándolas cuando existe intención dolosa y cuando el hecho es cometido por funcionarios públicos se penaliza con la inhabilitación[162].

Al igual que el C.P.F., el Código penal de España regula este delito en el titulo denominado Revelación de secretos (artículo 197, 197 bis, 197 ter, 197 quater y 197 quinquies, del Título X "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio" en el capítulo I referido a "Del descubrimiento y revelación de secretos") lo que permite que ambas legislaciones se equiparen en cuestión al tipo penal y el bien jurídico tutelado.

Así, podemos ver que en la legislación Española el tipo penal corresponde al descubrimiento y revelación de secretos; mientras que el bien jurídico a proteger es la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, por los artículos 197, 197 bis, 197 ter, 197 quater y 197 quinquies.

Por su parte, el Título XIII en los artículos 264, 264 bis, 264 ter y 264 quater del Código Penal de España, el tipo penal es "De los daños" refiriéndose a aquellos que afecten el patrimonio y el orden socioeconómico, mientras que el bien jurídico que se centra a proteger son el patrimonio socioeconómico.

---

[161] Cámpoli, Gabriel Andrés, *Derecho penal informático en México,* México, Instituto Nacional de Ciencias Penales, 2004, p. 18.

[162] Téllez Valdés, Julio, *Derecho informático,* 3a ed., México, McGraw Hill Interamericana, 2009, p.178.

En cambio, lo que difiere con el C.P.F es que en el tipo penal corresponde solamente al acceso ilícito a sistemas y equipos de informática, y el bien jurídico tutelado es la información contenida en esos sistemas y equipos de informática ante ataques que la modifiquen, destruyan o provoquen su perdida.

Así pues, Nava Garcés nos dice que: hemos visto con antelación que nuestro Código Penal Federal ubicó, como el español (en una parte) a los delitos informáticos en el capítulo referente a la revelación de secretos, tal vez porque con una frecuencia inaudita se da el acceso ilegal a un sistema de información[163].

Ahora bien, procederemos a hacer un análisis literal de estos artículos del Código Penal Español, para señalar las similitudes y diferencias que presenta con la legislación del Código Penal Federal de México, con el propósito de comprender mejor ambas legislaciones y así buscar mejorar el derecho penal vigente.

El artículo 197 párrafo segundo del Código Penal Español señala que: al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

La punibilidad que establece este artículo es de uno a cuatro años de prisión y multa de doce a veinticuatro meses; iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere, o utilice en perjuicio del titular de los datos o de un tercero.

Conforme a lo reglamentado, la falta de consentimiento es una conducta punible tanto las mencionadas anteriormente (apropiación e interceptación) como el acceso a los datos, con lo que se está ampliando el ámbito de seguridad jurídica al tipificar como delios conductas que implican abusos informáticos contra la libertad informática[164].

---

[163] Nava Garcés, Alberto Enrique, Análisis de los…, *cit.,* p. 113.
[164] Menéndez Mato, Juan Carlos y Gayo Santa Cecilia, Mª Eugenia, *Derecho e informática ética y legislación,* España, J M Bosch editor, 2014, p. 322.

Siguiendo con el análisis al artículo 197 del Código Penal de España, notamos que tiene la finalidad de proteger los datos informáticos reservados de carácter personal o familiar, ante probables ataques informáticos realizados por personas que sin autorización utilice o los modifique los datos informáticos contenidos en el sistema, pero, asimismo, el mencionado numeral carece de las conductas destruir, conocer o copiar información, tal como el C.P.F. si las regula.

Pero contrario, en la legislación mexicana podemos encontrar vaguedades, por ejemplo, el C.P.F no específica en forma clara en los artículos 211 bis 1 al 211 bis 7 la conducta de ocasionar daño a los datos informáticos de carácter personal o familiar, solo se refiere, con la expresión de ocasionar daño a la información pero no señala a qué tipo de información es la tutelada.

Además, se establece en el apartado 3 del artículo 197 del Código Penal de España regula diversas circunstancias agravantes de la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Abeledo nos dice: aquí es importante conocer que las mismas penas serán impuestas a aquel que, conociendo la ilicitud, revele a terceros la información intima descubierta aunque no haya participado en el descubrimiento. Por eso hay que ser muy críticos con lo que difundimos en nuestros medios sociales y sitios web[165].

Es decir, que si los datos informáticos (los que son protegidos de carácter personal o familiar) obtenidos se difunden, revelan o ceden a terceros, se agrava la pena y se castiga al responsable con la misma penalidad porque llegaría a afectar la intimidad y la propia imagen del dueño de esos datos.

Conjuntamente a lo anterior, en México tampoco se regula lo estipulado por el apartado 4 de este mismo artículo del Código Penal de España, el cual reglamenta otra agravante para los sujetos activos en calidad de garantes, al

[165] Abeledo Díaz, Miguel Ángel, *Aspectos legales de los negocios online*, España, Wolters Kluwer, 2012, p. 230.

mencionar que si los responsables del delito son personas encargadas o responsables de ficheros, soportes informáticos, electrónicos o telemáticos o registros, para este delito la pena será de tres a cinco años de prisión.

De igual manera, el C.P.F carece de lo contemplado por el apartado 5 del artículo 197 del Código Penal de España, al señalar que si los datos informáticos de carácter personal revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la victima fuere menor de edad o una persona con discapacidad, se le impondrán las penas previstas en su mitad superior, es decir, su punibilidad seria de dieciocho meses a seis años de prisión.

Por el contrario el apartado 6 del artículo 197 del Código Penal de España, se asemeja parcialmente con el artículo 211 bis 7 del C.P.F de México al señalar que si los hechos se realizan con fines lucrativos, se aumentará hasta en una mitad, y para España se impone la pena prevista en su mitad superior, es decir, la punibilidad seria de cuatro a siete años de prisión.

Por otro lado, al igual que el C.P.F., el Código Penal España expresa en su legislación las conductas correspondientes a utilizar, modificar y alterar información datos contenidos en sistemas o equipos informáticos, de forma similar a lo estipulado por el artículo 211 bis 1 del C.P.F.

Además, se establece una significativa diferencia en cuestión a las penalidades para este tipo de conductas antijurídicas, en la legislación española la penalidad de prisión es de uno a cuatro años y multa de doce a veinticuatro meses; y en México la penalidad es de seis meses a dos años de prisión y de cien a trescientos días multa, por lo que podemos ver que España es un poco más severo al aplicar penalidades más altas para quien realice el tipo penal.

El Código Penal de España al igual que el C.P.F. regula la conducta de acceso ilícito a sistemas y equipos de informática, por su parte el Código Penal de España en el artículo 197 bis lo regula de esta manera:

El que por cualquier medio procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda, o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Como se puede observar, al C.P.F le falta precisar ciertos actos que son importantes para determinar la conducta delictuosa, y de las que se está dejando un vacío legislativo por no contemplarlos, tal es el caso del acto de facilitar el acceso de una persona a otra a un sistema de información; y el que el sujeto activo se mantenga en el sistema informático en contra de su voluntad.

Por otro lado, al C.P.F también le falta regular la conducta contemplada en el artículo 197 bis párrafo segundo del Código Penal de España, mismo que establece:

El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte trasmisiones no púbicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

En cambio, el artículo 197 ter del Código Penal de España se equipara con el artículo 211 bis 7 del Código Penal Federal de México al establecer una agravante a este delito si los datos informáticos obtenidos se adquieran para su uso en provecho propio o ajeno.

Asimismo, en México tampoco no se contempla lo señalado por el artículo 197 quater, mismo que establece: si los hechos descritos en este capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

De esta manera, podemos ver que México no prevé este tipo de actos, contrario a España, que lo establece como agravante a las penas que se imponen

para este tipo de delito, lo que conlleva que México debe de comparar si es adecuado o no contemplarlo también en el Código Penal Federal.

Aunado a lo anterior, el C.P.F no regula lo estipulado por el artículo 197 quinquies, que establece: de acuerdo con lo establecido en el artículo 31 bis del Código Penal de España, la responsabilidad penal a personas que sean representantes legales de la que haya comisionado una de las conductas anteriormente descritas por el articulo 197 como delito; por lo que se le impondrá una pena de multa de seis meses a dos años.

Al analizar el código penal de España notamos que el Código Penal Federal de México carece de actos que si están regulados por el Código Penal de España, lo que conlleva a determinar que en México existen omisiones legislativas que conllevan a crear un amplio vacío en la ley acerca de actos no tipificados que pueden ser parte de un delito.

> Es necesario tener en cuenta que en nuestro derecho rige el principio de prohibición analógica en materia penal, por lo que se consideran comprendidas sólo aquellas conductas que encajen perfectamente en el tipo penal existente, siendo ello una derivación del principio de legalidad, que posee el raigambre constitucional[166].

Por lo tanto, si no se regulan este tipo de acto como delito, no se puede responsabilizar al autor por un hecho que cometió porque este mismo, no se encuentra plasmado en una ley previa, es por ello, la necesidad de contemplar todos los actos lesivos como delitos por el derecho escrito.

Por otro lado, dejando atrás los artículos 197 al 197 quinquies del Código Penal de España, también se regula a los delitos informáticos en el título XIII denominado delitos contra el patrimonio y contra el orden socioeconómico, en el capítulo IX denominado de los daños, correspondiente a los artículos 264, 264 bis, 264 ter y 264 quater.

---

[166] Hocsman, Heriberto Simón, *op. cit.,* pp. 285 y 286.

Aquí podemos notar una diferencia entre el Código Penal de España y el C.P.F., en cuanto a que en México, solo se regula la aparición del delito de Acceso ilícito a sistemas y equipos de informática, en un solo título (Revelación de secretos y acceso ilícito a sistemas y equipos de informática) mientras que el Código Penal de España lo regula en dos títulos por separado en atención a los diversos bienes jurídicos que tutelan.

Por lo que se refiere a la regulación del Delito de Daños, el Código Penal de España ha dado carta de naturaleza a los daños informáticos y al sabotaje informático, puesto que el artículo 264 contempla "los daños sobre los datos o programas" y "los ataques que impidan que un sistema funcione correctamente"[167].

El artículo 264 del Código Penal Español nos dice que: el que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

Luego entonces, surge una nueva similitud entre los ordenamientos jurídicos de España y México acorde a esta institución, al señalarse también en los artículos 211 bis 1 al 211 bis 7 del C.P.F. la descripción a las conductas de sin autorización, destruir, alterar, borrar y dañar información de documentos electrónicos al igual como se señala en el Código Penal de España.

También, la legislación penal Española establece una punibilidad más elevada al sancionar este tipo de delito de seis meses a tres años de prisión, lo que en México es de seis meses a dos años de prisión, por lo que podemos apreciar que España otorga más rigurosidad de penalidad en su legislación.

En lo que varía, es que en el mismo artículo 264 se establece un listado de actos que agravan la pena de dos a cinco años, mismos que el C.P.F no establece

[167] Menéndez Mato, Juan Carlos y Gayo Santa Cecilia, Mª Eugenia, *op. cit.,* p. 328.

como agravantes, ni como actos para el propio delito de acceso ilícito a sistemas y equipos de informática.

El listado de agravantes comprende estos actos: cuando el delito sea cometido dentro de una organización criminal; se hayan dañado de especial gravedad o afectado a un número elevado de sistemas informáticos; los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro para la seguridad del Estado de la Unión Europea o de un Estado Miembro de la Unión Europea.

Analizando el Código Penal de España, nos encontramos que este mismo no regula como tipo penal el delito de acceso ilícito a sistemas y equipos de informática como se regula en México, sólo se menciona de forma breve la no autorización al sistema pero tendiendo al bien jurídico de afectar en contra de la intimidad, a la propia imagen, y en contra del patrimonio, más no para la misma información contenida en los sistemas.

Por otra parte, el artículo 264 del Código Penal de España establece penalidad de prisión de seis meses a tres años para quien sin autorización y de manera grave, obstaculice o interrumpa el funcionamiento de un sistema informático ajeno.

También, a la legislación mexicana le falta regular la disposición anterior, ya que en el artículo 211 bis 2 párrafo cuarto del C.P.F. se agrava la penalidad para quien obstruya, entorpezca, obstaculice, limite o imposibilite la impartición de justicia o para los registros relacionados con un procedimiento penal.

Lo anterior, conlleva a limitar la legislación mexicana acerca de este delito, pues solamente tienen protección jurídica los equipos y sistemas informáticos que se utilicen en la impartición de justicia perteneciente al Estado, contrario a la legislación española que se refiere a equipos de cualquier tipo.

Otra disposición de la que México carece, es lo contemplado por el artículo 264 ter del Código Penal de España, al regular la conducta de ocasionarle daño

para utilizarse en o facilitarle a terceros un programa informático o a una contraseña de un ordenador, un código de acceso o datos similares del sistema informático.

Por ende, los Códigos Penales de España y México no son completamente diferentes en la tipificación de este tipo de delito lo que conlleva a que ambas legislaciones son parcialmente armónicas, porque regulan conductas que llevan al hecho delictuoso de la misma manera. Sin embargo al Código Penal Federal de México le falta muchas disposiciones en los tipos penales, supuestos comprendidos en el delito informático, conductas ilícitas, y agravantes, mismas que el Código Penal de España si regula, por lo que se debe de tomar en cuenta las diferencias que estos presentan para complementar nuestras leyes y así perfeccionar los vacíos y omisiones legislativas existentes, para evitar atipicidades y la impunidad.

## II. CIBERCRIMINALIDAD, POLICÍAS CIBERNÉTICAS Y POLÍTICA CRIMINAL EN EL ÁMBITO INTERNACIONAL

### 1. *Cibercriminalidad y policías cibernéticas frente a la comisión de los delitos informáticos en el ámbito internacional*

> Al respecto, Rivas Mayett expresa, muchos Estados ya han creado dependencias de delitos informáticos e inclusive han preparado diversos manuales con instrucciones técnicas, forenses y de procedimiento sobre la manera de llevar a cabo una investigación para reducir la perdida de pruebas y garantizan la admisibilidad de estas ante los tribunales[168].

En complementación a lo referido anteriormente podemos sumar que países como España, Perú, Chile, Estados Unidos, Reino Unido, Colombia, Francia, Alemania y México, por mencionar algunos, se han propuesto la tarea de crear organismos punitivos especializados en investigar y actuar en contra del fenómeno presente de la cibercriminalidad (entendidos estos mismos como policías cibernéticas).

[168] Rivas Mayett, Diana, *Cibercriminalidad en México,* México, Servicio express de impresión, 2012, p. 121.

A su vez, Romeo Casabona expresa: el cibercrimen se define como conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen en su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar bienes jurídicos diversos de naturaleza individual o supraindividual[169].

En ese sentido, la cibercriminalidad se conforma por las diferentes modalidades antijurídicas de la informática, por ejemplo: el sabotaje informático, los virus informáticos, la modificación de datos, el acceso no autorizado a equipos y sistemas informáticos, los gusanos informáticos, las bombas lógicas, la manipulación informática, el *hacking*, el *cracking* entre otras más.

Los efectos de la cibercriminalidad recaen en los bienes jurídicos de las personas, como la privacidad, la intimidad de las personas y el patrimonio económico con las modalidades de daño y fraude informático, afectando a la información contenida en sistemas y equipos informáticos.

De este modo Palazzi manifiesta, el delito informático es más difícil de investigar que el delito tradicional porque es novedoso, escapa los cañones tradicionales, los cuerpos policiales y tribunalicios no están preparados para investigar y detectar técnicas novedosas y el propio delito suele no dejar rastros, en el ambiente digital no quedan huellas a simple vista[170].

La forma en la que actúan los ciberdelincuentes es con la finalidad de no ser localizados, por lo que operan con sistemas electrónicos que contienen una tasa muy alta de seguridad informática, lo que a la vez les permite no dejar rastros y esconder sus rostros detrás de los ordenadores.

[169] Romeo Casabona, Carlos María, "De los delitos informáticos al crimen, Una aproximación conceptual y político-criminal", en Romeo Casabona, Carlos María (coord.), *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Editorial Colmares, España, 2006, p.9.
[170] Palazzi, Pablo Andrés, *Delitos informáticos, Argentina,* AD-HOC Buenos Aires, 2000, p. 70.

El no dejar rastro alguno es una característica de esta criminalidad. El delincuente informático hace dos cosas antes de dejar la escena del crimen: la primera, es eliminar todos los archivos que ha usado, la segunda, es modificar los archivos de movimiento y actividades, y borrar todos los signos de entrada[171].

De esta manera, podemos ver que el ciberdelincuente es una persona astuta con mucha pericia en los sistemas y equipos informáticos, es por ello, que este delito es difícil de investigar, lo que conlleva la afectación de los bienes jurídicos de las víctimas no se reparen si no se encuentra al responsable.

> Rivas Mayett destaca que, el anonimato que brindan los delitos informáticos provoca a la víctima la sensación de que la justicia penal no podrá dar con el responsable del ataque en su contra, asimismo siente que se enfrenta a un ser "invisible" frente a cuyos ataques solo queda resignarse, por lo que pocas veces denuncia los hechos[172].

Con ello, planteamos una cuestión ¿Qué es lo que hace que estos delitos sean difíciles de investigar? La respuestas son muy fáciles, primera: al ser un delito complejo, es decir, la persona que lo comete es un sujeto cualificado, es también un delito de abocarse a su persecución, pues no cualquier organismo público punitivo lo puede hacer, para esto se necesitan de policías cibernéticas, con personal especializado en equipos informáticos, sistemas informáticos y en redes;

Y la segunda respuesta es que al ser estas conductas mayormente cometidas con la ayuda de la Internet forman a ser interestatales, es decir, se pueden cometer en un país y pueden tener efectos en otro si así se desea, o si así se requiere para lograr el objetivo, lo que ayuda a que este delito sea difícil de investigar es que no en todos los países cuentan con policías cibernéticas, por lo que, o no se investiga (y si se investiga no se hace de la manera adecuada por falta de conocimientos y pericia en la rama de la informática) o se le pierde el rastro al ciberdelincuente.

---

[171] Rivas Mayett, Diana, *op. cit.,* p. 104.
[172] *Ibídem,* p.30.

Conforme a las hipótesis planteadas, sugerimos que estas serían las dos bases más importantes que se deben de atender para hacer frente a esta problemática internacional, ya que se requiere de la creación de unidades especializadas que actúen internacionalmente para que se dediquen a combatir el cibercrimen y a investigar los casos de delitos informáticos que se presentan.

> Así pues para Lira Arteaga, la investigación forense aplicada a las Tecnologías de la Información y la Comunicación (TIC), es una rama de la criminalística que se aplica en la búsqueda, tratamiento, análisis y preservación de indicios relacionados con una investigación, en donde, tanto el equipo de cómputo y/o telecomunicaciones han sido utilizados como fin o como medio para realizar una acción presuntamente delictiva[173].

Analizando el concepto anteriormente citado, podemos apreciar que para lograr una investigación forense informática efectiva en el ámbito internacional, se necesita de Policías Cibernéticas que actúen en sus países para que realicen la investigación, recopilación de pruebas y a su vez, prevención de los ciberdelitos.

Por ende, la ausencia de Policías Cibernéticas hace que el delito informático sea uno de los más difíciles de comprobar, pues también se tiene que determinar la ubicuidad territorial del mismo y de sus autores, de igual forma se tiene que seguir la persecución aunque se traspasen los límites territoriales.

Como consecuencia de la posibilidad de alejamiento espacial, y gracias a la Internet, el distanciamiento entre el lugar donde se sitúa el autor de la conducta, o donde ésta se lleva acabo, y la del lugar donde se producirán sus consecuencias constituye una situación que redunda en la superación de los límites nacionales[174].

---

[173] Lira Arteaga, Óscar Manuel, "Cibercriminalidad", en García Ramírez, Sergio y González Mariscal De, Olga Islas (comps.), *Derecho penal y criminalística XII jornadas sobre justicia penal,* México, UNAM, Instituto de Investigaciones Jurídicas, Instituto de la Formación de la Procuraduría General de Justicia del Distrito Federal, 2012, p. 176.

[174] Balmaceda Hoyos, Gustavo, *El delito de estafa informática,* Colombia, Leyer Editorial, 2009, p. 69.

Debido a lo anterior, es que se plasma la necesidad de contar con Policías Cibernéticas en los países, y hasta que no se cuente con una cooperación internacional que actué efectiva y eficazmente en contra de los delitos informáticos, la cibercriminalidad no se reducirá y así será muy difícil contrarrestar esta problemática que afecta la comunidad internacional.

Asimismo en el ámbito internacional la Organización Internacional de Policía Criminal (INTERPOL) es el máximo organismo encargado de coadyuvar con las tareas policiales de los países, actuando estratégicamente ante amenazas de delitos que puedan organizar graves daños a un grupo de países como tal es el caso de la cibercriminalidad.

> La INTERPOL expone que el cibercrimen es un área de crímenes de rápido crecimiento. Cada vez más delincuentes están explotando la velocidad, la comodidad y el anonimato de la Internet para cometer una amplia gama de actividades delictivas que no conocen fronteras, ya sean físicas o virtuales, causan daños graves y representan amenazas muy reales para las víctimas en todo el mundo[175].

Debido a la preocupación de la cibercriminalidad que rodea al mundo, la INTERPOL ha creado un departamento especializado en delincuencia informática, el mismo se encuentra conformado por un grupo de expertos en esta rama encargados de cooperar internacionalmente en contra de los ciberdelitos.

> INTERPOL está comprometido con la lucha mundial contra del cibercrimen y los delitos cibernéticos. La mayoría de los delitos cibernéticos son de naturaleza transnacional, por lo tanto, INTERPOL, es el socio natural de cualquier agencia de aplicación de la ley que desee investigar estos tipos de delitos a nivel cooperativo. Al trabajar con la industria privada, INTERPOL

[175] https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime

puede proporcionar a la policía local inteligencia cibernética enfocada derivada de la combinación de insumos a escala global[176].

Conforme a lo esgrimido se considera que las actividades realizadas por este organismo internacional son de gran ayuda para los países, más aún para aquellos en donde no se cuenta con una policía cibernética, o bien, si la tiene, no cuenta con el personal o el equipo especializado para llevar a cabo esta labor.

Por otra parte, ahora plantearemos algunas formas en la que países como España, Chile, Estados Unidos, Reino Unido, Colombia, Francia, Alemania y México hacen frente a los delitos informáticos a través de sus Policías Cibernéticas y la manera en la que estas se conforman o como se desempeñan.

> España cuenta con el Grupo de Altas Tecnologías de la Guardia Civil y con la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, constituida en marzo de 2000 a partir de la antigua Brigada de investigación de la Delincuencia Tecnológica de la Policía Nacional. Ambos tienen encomendada la función de vigilancia de los sistemas informáticos y la investigación y persecución de los delitos informáticos[177].

En España como se dijo anteriormente, se cuenta con dos unidades especializadas de apoyo para hacer frente a la cibercriminalidad, en atención a vigilar los sistemas informáticos y de encargarse al campo de la investigación forense para responsabilizar a sus autores.

En atención a esto, consideramos que España es un país comprometido con la seguridad de su nación, así como también con la comunidad internacional, al no solamente legislar estas conductas delictivas en su Código Penal sino también en formar una unidad especializada que atiende a este delito.

---

[176] Idem.

[177] Marín Peidro, Lucia, *Los contenidos ilícitos y nocivos en Internet,* España, Fundación Retevisión, 2000, p. 124.

Unos meses después de España, Chile crea su propia Policía Cibernética, en sus funciones plantea protección jurídica a una amplia gama de delitos informáticos, no solo los que atentan contra la información, sino también aquellos que van en contra el patrimonio, la intimidad y, la libertad y seguridad sexual de menores de edad, mismos que se pueden agredir por los medios informáticos.

> La Brigada de Investigaciones del Cibercrimen de la Policía Investigadora de Chile, consciente de los avances tecnológicos en el ámbito delincuencial, creó en octubre de 2000 la Brigada de Investigación del Cibercrimen, Unidad Especializada en la Comisión de Delitos vía Internet como amenazas, estafas, falsificación, pornografía infantil y delitos informáticos propiamente[178].

Chile como país latinoamericano se ha preocupado por responder internacionalmente al fenómeno de la cibercriminalidad, por lo que podemos ver que el enfoque de su Policía investigadora contra el cibercrimen se encuentra también en inspeccionar las conductas que se realizan por medio de la Internet.

> Por otro lado Paloma Parra señala que el 26 de enero de 2004 la FTC (*Federal Trade Commission*, "Comisión Federal de Comercio") de Estados Unidos llevó a juicio el primer caso contra un *Phisher* sospechoso. El acusado, un joven adolescente de California, supuestamente creó una página *web* con diseño que aparentaba ser la página de *América Online* para poder robar números de tarjetas de crédito[179].

Estados Unidos como podemos ver es un país comprometido con la comunidad internacional al poner en marcha su policía cibernética, la misma está actuando en contra del cibercrimen al llevar a proceso jurisdiccional a *hackers* y *crakers* por delitos cometidos por medios informáticos que afectan al bien jurídico del patrimonio.

---

[178]Nava Garcés, Alberto Enrique "Internet en América latina y su regulación", en Nava Garcés, Alberto Enrique (coord.), *El derecho en la era digital,* México, Porrúa, 2013, p. 177.
[179] Paloma Parra, Luis Orlando, *op, cit.,* p. 120.

En 1999 atacaron los virus Melissa, Chernovyl, Explore Zip, y Bubbleboy; en el año 2000 el virus I LOVE YOU causó daños, en algunos casos irreparables. Los fraudes en Internet aumentaron en ese mismo año, se presentaron los casos en el Servicio de Crímenes Comerciales de la Cámara de Comercio Internacional[180].

En consecuencia, podemos ver que los virus son una problemática catastrófica que afecta internacionalmente a los datos contenidos en sistemas y equipos informáticos, y como tienen el carácter de ser infecciosos se van propagando por los diversos equipos y sistemas informáticos provocando una afectación en masa.

Los virus son agentes de disturbios que afectan en distinto grado a los equipos informáticos y a sus dueños como víctimas provocándoles importantes pérdida ya sean económicas y de información. Tienen la capacidad de alterar, borrar, o destruir la información que se encuentra en la computadora[181].

Dicho de esta manera, los virus informáticos tienen el objetivo de provocar pérdidas en la información de los sistemas, y cuando estos afectan al patrimonio de empresas internacionales interviene la Cámara de Comercio Internacional para brindar protección a dichas empresas.

En junio de 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica de *phishing*, en un caso conectado a la denominada *Operarition Firewall* del Servicio Secreto de los Estados Unidos, que buscaba sitios web notorios que practicaban el *pshishing*[182].

Estados Unidos y el Reino Unido están colaborando conjuntamente para contrarrestar los casos de la modalidad del *pshishing* que en los últimos años se han presentado en sus países y que traspasan límites territoriales, asimismo podemos ver que estos se han ayudado para frenar el cibercrimen.

---

[180] Azaola Calderón, Luis, *Delitos informáticos y derecho penal,* México, Ubijus Editorial, 2010, pp. 46 y 47.
[181] Luz Clara, Bibiana, *Manual de derecho informático*, Argentina, Editorial jurídica Nova Tesis, 2001, p. 119.
[182] *Idem.*

También en Colombia los ciberdelincuentes están siendo advertidos y judicializados por la Ley 1273 de enero de 2009, gracias a los elementos materiales probatorios y la evidencia física que dejan al incursionar en las acciones contrarias a derecho[183].

De esta manera en Colombia también se está actuando en contra de la cibercriminalidad, lo que ayuda que más países latinoamericanos se sumen a la cooperación internacional en el ámbito de responsabilizar con la ayuda de la informática forense a los autores de este delito.

> En países como Francia, España, Alemania, entre otros, la información (de los medios de prueba) se almacena hasta por un año, permitiendo así que responsables de realizar investigaciones relacionadas con este tipo de conductas cuenten con el tiempo suficiente para evitar que la información que permite identificar al ciberdelincuente a través de Internet se pierda[184].

En estos países se practica para este tipo de delitos, el resguardo de los medios de prueba de próximos sabotajes que pudieran ocurrir, para así evitar que se ocasione una perdida (total o parcial) o modificación de dichos medios de prueba, con esta disposición se pretende asegurar el éxito de la investigación.

En consecuencia, hasta este momento hemos abordado el tema de las Policías Cibernéticas a nivel internacional, ahora con el propósito de ampliar nuestro conocimiento en el tema procederemos a señalar a las policías cibernéticas en México; ¿cómo están conformadas?, ¿cuáles son sus funciones?, ¿Qué estados de la República Mexicana cuentan con esta unidad especializada?, en ese sentido iremos respondiendo a cada una de estas interrogantes.

> En México, tomando en cuenta la dificultad probatoria de los delitos informáticos, se ha formado la Coordinación Interinstitucional de Combate a Delitos Cibernéticos, formado por: la Presidencia de la Republica, la Policía

[183] *Ibidem*, p. 3.
[184] Lira Arteaga, Óscar Manuel, "Cibercriminalidad", en García Ramírez, Sergio y González Mariscal De, Olga Islas (comps.), *op. cit.,* p. 172.

Federal Preventiva, el Centro de Investigación y Seguridad Nacional, la Secretaría de Defensa Nacional, la Secretaría de Marina y la Secretaría de Seguridad Publica (a través de la Policía Federal Preventiva)[185].

La Coordinación Interinstitucional de Combate a Delitos Cibernéticos, posteriormente denominada como policía de ciberdelincuencia preventiva, o conocida mayormente como Policía Cibernética, fue la primera unidad especializada en México en combatir los delitos informáticos, después otros estados de la República Mexicana se han interesado en crear estas nuevas unidades especializadas para que actúen en su jurisdicción.

Asimismo, se encuentra la organización *DC México* y la cual es una muestra de agrupaciones que auxilian en sus actividades a la Policía Cibernética en la función investigadora, la cual es encabezada por la Secretaría Técnica de la Policía Federal Preventiva que inicia sus funciones el 9 de diciembre de 2002. Su objetivo es garantizar la seguridad en la navegación en la red, así como combatir los ilícitos provocados por el uso de sistemas de cómputo[186].

A pesar de que existe este organismo para el auxilio de la Policía Cibernética poco se habla del mismo, no obstante sus funciones son muy importantes pues se encarga del ciberpatrullaje en la Internet con el objetivo de la prevención de los delitos informáticos. Actualmente con la nueva reforma constitucional publicada en el D.O.F el 26 de marzo de 2019, la Policía Federal forma a ser parte de la Guardia Nacional, lo que conlleva a la prevención de este delito a nivel nacional.

En la actualidad tanto la Policía Cibernetica como DC México, para lograr cierta cooperación internacional, trabajan conjuntamente con los siguientes organismos: *US Customs Cybersmuggling Center (C3),* Servicio Secreto de los EUA, *National Center for Missing & Expoiled Children*, Brigada Tecnológica de España[187].

---

[185] Nava Garcés, Alberto Enrique, *Análisis de los…, cit.,* p. 106.
[186] Rivas Mayett, Diana, *op. cit.,* pp. 148 y 149.
[187] *Idem,* pp. 150.

De esta manera, la Policía Cibernética de México busca colaborar internacionalmente con diversos organismos de Estados Unidos y España, esto con el propósito de hacer frente al fenómeno de la cibercriminalidad y de resguardar al país de ataques a los sistemas de información que puedan penetrarse en México.

El problema más acentuado que plantea la efectividad de la persecución penal de los delitos cometidos a través de la red, consiste en la determinación del lugar y tiempo de comisión del delito. La sociedad de la información ha conducido a la irrelevancia de los límites territoriales[188].

En consecuencia lo se ha buscado lograr en estos últimos años en México, es establecer Policías Cibernéticas en todas las entidades del país, el proceso ha sido lento pero constante, por ello, procederemos a ver en qué entidades federativas ya se encuentran trabajando estas unidades especializadas.

De esta manera, los estados que cuentan ya con una unidad de forense informática especializada son el estado de México[189], Jalisco[190], Querétaro[191], Veracruz[192], Yucatán[193], Baja California Sur[194], Chiapas[195], Chihuahua[196], Coahuila[197], Colima[198], Guanajuato[199], Guerrero[200], Michoacán[201], Morelos[202],

[188]Romeo Casabona, Carlos María, "De los delitos informáticos al crimen… *cit.,* p. 31 y 32.
[189] http://sseguridad.edomex.gob.mx/seguridad-publica-transito/policia-cibernetica
[190] https://fge.jalisco.gob.mx/policia-cibernetica
[191] http://www.eluniversalqueretaro.mx/portada/01-07-2014/logros-de-policia-cibernetica
[192]http://www.veracruz.gob.mx/seguridad/atiende-policia-cientifica-casi-300-casos-de-delitos-ciberneticos/
[193]http://www.fge.yucatan.gob.mx/rt.php?seccion=comunicacionsocial&subseccion=noticias&accion=detalles&id=1400&titulo=polic&iacutea-cibern&eacutetica-de-la-fge-llama-a-usar-herramientas-de-privacidad
[194] http://www.pgjebcs.gob.mx/cibernetica/
[195] https://www.sspc.chiapas.gob.mx/noticias/vgwXuLiUSoc-3D-
[196] http://fiscalia.chihuahua.gob.mx/inicio/?page_id=468
[197] http://www.milenio.com/policia/diez-agentes-integran-policia-cibernetica-coahuila
[198] http://www.colima-estado.gob.mx/2016/index.php/portal/noticia/6760017269251293761
[199] https://www.facebook.com/PoliciaCiberneticaGto/
[200] http://uadcgro.blogspot.mx/p/denuncias.html
[201]http://www.nuestravision.com.mx/index.php/component/videoflow/play/65233-crean-unidad-de-policia-cibernetica-en-michoacan
[202] http://www.cesmorelos.gob.mx/?page_id=7619

Nayarit[203], Puebla[204], San Luis Potosí[205], Tabasco[206], Oaxaca[207], Hidalgo[208],Tamaulipas[209], Tlaxcala[210], Baja California[211], Campeche[212], Durango[213].

Así, podemos ver que veinticinco estados de la República Mexicana ya tienen integrado en su organización estatal una Policía Cibernética, falta determinar qué tan eficaces son estos organismos policiales, para ello es preciso determinar cuáles son sus funciones para ver si estas son eficientes a lo que se requiere.

Entre sus actividades está el ciberpatrullaje en la red mediante *software* convencional para el rastreo de *hackers,* sitios de Internet, comunidades y *chats rooms* en los que se promuevan la pornografía y el turismo sexual infantil. Asimismo, se utiliza Internet como instrumento para detectar a delincuentes[214].

Para los estados del país donde ya se cuentan con estas unidades de especialización contra los ciberdelitos, sus funciones son principalmente atender denuncias, investigar y procesar el cibercrimen, y también se dedican en vigilar constantemente los sitios web y las redes sociales.

Otra de las funciones que hacen las Policías Cibernéticas es formar pláticas informativas en centros escolares e instituciones con el objetivo de advertir sobre los delitos y peligros que se cometen a través de la Internet, así como la forma de prevenirlos creando una cultura de autocuidado y civismo digital[215].

---

[203]http://nnc.mx/articulo/Policiaca/detenido-por-amenazar-en-facebook-de-una-masacre-en-la-prepa-1/1486657578

[204] http://ssp.puebla.gob.mx/index.php/delitos-ciberneticos

[205]http://congresosanluis.gob.mx/content/atenci%C3%B3n-delitos-cibern%C3%A9ticos-por-autoridades-especializadas

[206] http://www.fiscaliatabasco.gob.mx/Contenido/UnidadDelitosInformaticos

[207] https://diario.mx/noticias/television/programas-de-noticias/primer-policia-cibernetica-en-oaxaca/

[208] http://s-seguridad.hidalgo.gob.mx/?p=4037

[209] http://www.milenio.com/policia/entra-en-operacion-policia-cibernetica

[210] http://www.e-tlaxcala.mx/nota/2017-05-28/gobierno/quedo-creada-la-division-cientifica-y-unidad-de-policia-cibernetica-en

[211] https://www.20minutos.com.mx/noticia/329809/0/policia-de-baja-california-tiene-nueva-unidad-cibernetica/

[212] http://www.ssp.campeche.gob.mx/index.php/historico-boletines/345-20-02-2018-alerta-policia-cibernetica

[213] https://www.elsiglodetorreon.com.mx/noticia/1348366.unidad-cibernetica-inicia-operaciones.html

[214] Nava Garcés, Alberto Enrique, "Internet en América latina y su regulación", *cit.,* p. 166.

[215] http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

El civismo digital es una función que realizan las Policías cibernéticas la cual es muy importante, en el sentido de preparar a la sociedad de la prevención de los delitos informáticos, al dar recomendaciones para evitar la infección de algún virus o bomba lógica, que pueda dañar la información de los sistemas informáticos.

Ante esto, la Policía cibernética del estado de México, para hacer efectiva su labor de protección ciudadana ha emitido constantemente alertas cibernéticas dirigidas a la sociedad, como un mecanismo de control preventivo difundiéndolas en redes sociales como *Facebook y Twitter.*

La más reciente alerta, fue por el virus informático denominado *Ransonware WannaCry* con fecha del 12 de mayo de 2017[216], el cual consiste en encriptar la información contenida en el sistema operativo y/o archivos de las computadoras para solicitar montos de dinero ante su rescate, es decir, como si fuera un secuestro de datos.

Aunado a lo anterior, los estados que ya tienen aprobado el dictamen de creación de la unidad especializada en contra de delitos informáticos pero que aún no tienen ni su organización ni la fecha de inicio para actividades son los estados de Nuevo León[217], Zacatecas[218], Aguascalientes[219], Quintana Roo[220] faltará ver para cuando ponen en marcha estos proyectos ya aprobados.

Por otro lado el 23 de marzo de 2018 el estado de Sonora[221], informó a través de su página web oficial la preparación de su Policía Cibernética con dieciséis elementos especializados, los mismos, se encuentran en proceso de capacitación para integrar la División de Policía Cibernética del estado, faltara ver la fecha en la que entre en funciones.

---

[216] http://data.ssp.cdmx.gob.mx/documentos/ciberdelincuencia/infografias/48_Infografia.pdf
[217] http://www.milenio.com/policia/tendra-nl-ciber-policias
[218] http://ntrzacatecas.com/2017/01/20/sin-precisar-creacion-de-policia-cibernetica/
[219] https://www.unotv.com/noticias/estados/aguascalientes/detalle/ya-construyen-cuartel-para-la-ciberpolicia-en-aguascalientes-525001/
[220] https://sipse.com/novedades/reclutamiento-elementos-aspirantes-policia-cibernatica-analisis-capacitacion-requisitos-examen-cancun-290372.html
[221] http://sspsonora.gob.mx/index.php/encuesta-de-satisfaccion-ciudadana/85-destacadas/512-se-prepara-sonora-para-contar-con-division-de-policia-cibernetica.html

Pero por el contrario, en el año de 2017 el estado de Sinaloa[222], se propuso como iniciativa al H. Congreso del Estado la creación de Policías Cibernéticas estatales, sin embargo al momento de discutir esta iniciativa fue rotundamente denegada por falta de presupuesto y por otras disposiciones más.

Debido a lo anterior, es importante tomar en cuenta que todos los estados del país deben de contar con su policía cibernética estatal para que cooperen nacionalmente en la persecución de estos tipos de delitos inmiscuidos en las redes de Internet.

Asimismo, podemos ver que en el país aún falta mucho por hacer, tanto para los estados que ya tienen aprobada la creación de Policías Cibernéticas y, más aún para los que las han rechazado las iniciativas, pues es de urgencia atender este fenómeno que afecta a la sociedad.

Y bien, conforme la pregunta, ¿Cómo denunciar un delito informático cuando un estado carece de una Policía Cibernética? para evitar la impunidad del cibercrimen la Comisión Nacional de Seguridad[223] (es un organismo de carácter público federal) se encarga de recibir las denuncias provenientes de todo tipo de conductas informáticas delictivas, para así sancionar a ciberdelincuentes.

Hoy en día, ante los ataques informáticos cometidos y conforme a las bases que anteriormente se describieron, podemos ver el estado de necesidad que presenta nuestro país al no tener establecido en todo su territorio unidades especializadas de policías cibernéticas que ataquen en la esencia de este problema.

2. *Política criminal internacional en los delitos informáticos*

Después de analizar la cooperación internacional; la legislación de Alemania, Francia y España; y los aspectos de la necesidad de las Policías Cibernéticas,

[222] https://www.debate.com.mx/culiacan/Sin-recurso-para-Policia-Cibernetica-diputados-20170630-0049.html

[223] http://www.delitosinformaticos.mx/que-es-un-delito-informatico/como-denunciar-delitos-ciberneticos-en-mexico/

inmersos en el contexto para la ayuda mutua en la prevención y persecución de los delitos informáticos en el ámbito internacional, procederemos a analizar la política criminal internacional que ha recomendado la ONU en sus Congresos Internacionales.

> Cita Triana nos dice que la política criminal, es el conjunto de respuestas que un Estado estima necesario adoptar para hacer frente a las conductas consideradas como reprochables o causantes de un perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción[224].

En este sentido, la política criminal es el pilar fundamental en el que se desarrollan las legislaciones, medidas, planes y estrategias con las que un Estado hace frente a la criminalidad dentro de su territorio, o bien, en el ámbito internacional para el apoyo con los demás países.

Son varios los factores que ayudan al legislador a tomar una decisión sobre el merecimiento de pena de una conducta. Unos son los factores normativos o de justicia; y otros los factores empíricos o de utilidad. Juntos constituyen la política criminal, es decir, las pautas a tener en cuenta por el legislador[225].

Asimismo el legislador toma como base los congresos internacionales que desarrolla la ONU cada cinco años desde el año de 1955[226], denominados Congresos de las Naciones Unidas sobre la Prevención del Delito y Justicia Penal, dado que en estos mismos se exponen dichos factores anteriormente mencionados.

En estos congresos se plantean temas a discutir que repercuten a la comunidad internacional, y la ONU elabora recomendaciones para que sus estados miembros creen su política criminal con el objetivo de buscar la prevención del delito tanto en su territorio como internacionalmente.

---

[224] Cita Triana, Ricardo Antonio *et. al.,* "¿Qué es la política criminal?", *Observatorio de política criminal,* Colombia, septiembre de 2015, sesión de trabajo n° 1, p. 3
[225] Muñoz Conde, *cit.,* p. 191.
[226] http://www.un.org/es/events/crimecongress2015/about.shtml

Aplicando estos congresos a los delitos informáticos, el 12º Congreso de las Naciones Unidas celebrado en Salvador de Bahía (Brasil) del 12 al 19 de abril de 2010, se desarrolló el tema del delito cibernético[227], como una novedad reciente en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia.

De la misma manera, en el 13º congreso celebrado en Doha (Qatar) del 12 al 19 de abril de 2015 (el Congreso más reciente) también se desarrolló el tema de los delitos informáticos aplicado al rubro de la ciberdelincuencia[228], con énfasis al fortalecimiento de las respuestas del delito y justicia penal frente a las formas de delincuencia en evolución y la cooperación internacional.

Dicho todo lo anterior, procederemos a analizar ambos congresos para conocer cuáles han sido las recomendaciones que ha emitido la ONU a sus Estados Miembros, y por último, analizaremos la política criminal que ha implementado el Estado mexicano como estrategia para la prevención de la cibercriminalidad.

> En el 12° Congreso se celebró un debate general acerca del tema "Novedades recientes en el uso de la ciencia y la tecnología por delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético", formularon declaraciones los representantes de China, Argelia, Canadá, Argentina, Estados Unidos, Arabia Saudita, Federación de Rusia, Alemania, Bostwana, Cuba, Chile, Unión Europea, Polonia, República de Corea, Azerbaiyán, México, Indonesia y Angola[229].

Como se aprecia, dieciocho países del mundo se han mostrado interesados en debatir esta problemática, incluidos entre ellos México y varios países el continente Americano, esto con el fin de buscar una solución al fenómeno de la cibercriminalidad en el ámbito internacional y buscar la prevención de este delito.

---

[227] http://www.un.org/es/conf/crimecongress2010/
[228] http://www.un.org/es/events/crimecongress2015/conference-programme.shtml
[229] Naciones Unidas, *12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal,* Salvador (Brasil), 2010, pp. 59 y 60.

En el debate se destacó el carácter transfronterizo del delito cibernético, la falta de conocimientos sobre el alcance del problema y las diferencias entre los sistemas nacionales. Se dijo que el delito cibernético era uno de los mayores problemas que afrontaban los órganos de aplicación de la ley[230].

Como lo mencionamos anteriormente, el delito informático es de naturaleza transfronterizo, es por ello, que todos los países del mundo deben de buscar adecuarse a cooperar internacionalmente con otros tanto en unificar las legislaciones y la política criminal, para así prevenir el aspecto de la cibercriminalidad tanto nacional como en el plano internacional.

> Diversos oradores informaron de las medidas adoptadas por sus gobiernos para combatir el delito cibernético, como la promulgación de legislación penal, la reglamentación de los cibercafés, iniciativas de creación de capacidad, campañas de sensibilización, el reforzamiento de los mecanismos para presentar denuncias y la protección de los grupos vulnerables[231].

Otro de los aspectos que se planteó en este Congreso, fue las diferencias de las legislaciones de los países que ya han tipificado estas conductas como delito (como ya hemos mencionado anteriormente en el tema de la cooperación internacional), también se señala, que es se suma importancia la cooperación internacional para responsabilizar a los ciberdelincuentes.

Se reconoció que los países en desarrollo eran los más vulnerables al delito cibernético. Los países desarrollados deberían aumentar urgentemente la asistencia para la creación de capacidad, en particular la destinada al personal de organismos de aplicación de la ley, los fiscales y los jueces[232].

En ese sentido, la ONU reconoce que los países en desarrollo son más vulnerables tal vez y porque le falta legislación, reglamentación e inspección en las redes informáticas, es por ello que los demás países deben de cooperar con estos.

---

[230] *Ibídem*, p.60.
[231] *Idem.*
[232] *Ibídem,* p. 62.

Por otro lado, también se da la recomendación de capacitar al personal de organismos como legisladores, fiscales y jueces, para que se actualicen con las situaciones novedosas y busquen estrategias para la prevención del ciberdelito.

Las recomendaciones que dio la ONU en este 12° congreso fueron:

1. Se convino en que el desarrollo de la tecnología suponía tanto beneficios como riesgos para la sociedad, y que la lucha contra el delito cibernético exigía una atención urgente. Se deberían analizar con especial atención los factores coadyuvantes y los nexos entre tecnología y el delito, a fin de elaborar estrategias eficaces[233].

Esta recomendación que platea la ONU para que la adopten los Estados Miembros en su política criminal nos parece muy importante, pues se deben de analizar los factores que influyen en la tecnología y en el delito al elaborar la política criminal que el Estado va a implementar, para que estas sean eficaces y prever las formas de prevención del delito.

2. Los estados deberían desarrollar una capacidad sostenible a largo plazo y fortalecerla. Los países en desarrollo requerirían con urgencia asistencia técnica en particular para la creación de capacidad y redacción de leyes, así como recursos materiales y expertos capacitados[234].

Esta otra recomendación es también muy importante, pues los Estados donde ya se tenga una política criminal sustentable al delito informático se debe de procurar que esta misma se refuerce para evitar la incidencia de este delito, de la misma manera, países en donde no se tenga con legislación aplicable para este tipo de conductas deben de tener asistencia para que las regulen de forma urgente.

3. La UNODC (Oficina de las Naciones Unidas Contra la Droga y el delito) debería seguir cooperando con las organizaciones pertinentes para prestar asistencia técnica a ese respecto, en particular teniendo en cuenta los

[233] *Ibídem,* p. 63.
[234] *Idem.*

programas de asistencia técnica y los instrumentos jurídicos de otras organizaciones intergubernamentales. Se debería estudiar con especial atención la posibilidad de elaborar un plan de acción para la creación de capacidad en el plano internacional[235].

Esta recomendación actualmente no ha sido acatada por parte de la UNODC en apoyar a México en su estrategia de política criminal en contra de la cibercriminalidad, en ese sentido, México ya ha elaborado un plan de Estrategia Nacional de Ciberseguridad (como lo veremos más adelante) en donde se toma en cuenta la importancia de la cooperación internacional, asimismo México si ha tomado en consideración las recomendaciones de la ONU al elaborar su política criminal.

4. Los Estados deberían hacer todo lo posible por intensificar la cooperación entre las instituciones nacionales, así como entre ellos y con el sector privado. Era preciso aumentar el intercambio de información y mejores prácticas entre los Estados mediante, por ejemplo, el fortalecimiento de las redes pertinentes[236].

En consecuencia a esta recomendación podemos referir que los Estados deben de trabajar conjuntamente tanto internacionalmente, como también, con las instituciones del sector privado con el objetivo intercambiar información que sea útil para prevenir la cibercriminalidad.

Como se aprecia, han sido varias las recomendaciones que ha emitido la ONU a los Estados Miembros en este 12° Congreso, estas mismas, son importantes para que los Países creen o perfeccionen la política criminal que van a adoptar para hacer la prevención de la cibercriminalidad. Ahora nos dirigiremos a analizar cuáles han sido las recomendaciones que emitió la ONU en el 13° Congreso.

[235] *Idem.*
[236] *Idem.*

En el 13° Congreso de las Naciones Unidas Sobre Prevención del Delito y Justicia Penal en Doha (Qatar), se desarrolló el seminario 3 denominado: El fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional[237].

Este seminario abarca tanto aspectos relacionados con la ciberdelincuencia como también, los del tráfico de bienes, puesto que estos dos delitos han ido en aumento en los últimos años, aun así, conforme a los objetivos de este trabajo de investigación solo nos limitaremos a analizar los aspectos de la ciberdelincuencia.

> Desde la década de 1960 muchos países han reconocido como delitos ciertos actos relacionados con la informática, como el uso no autorizado de sistemas informáticos y la manipulación de datos informáticos. Pero ha sido con la llegada de Internet que las tecnologías globalizadas de la información y de las comunicaciones han empezado a usarse para cometer delitos a escala internacional en forma de ciberdelincuencia que conocemos actualmente[238].

Sin duda, como ya lo hemos referido anteriormente, el carácter transfronterizo de los delitos informáticos se debe a la proliferación de la Internet por todo el mundo, esto es un factor para que en estas últimas décadas, este tipo de delitos valla en aumento.

Ahora bien, hay que destacar cuáles han sido las recomendaciones que dio la ONU en este 13° Congreso para hacer frente y prevenir la cibercriminalidad:

1. Los Estados Miembros pueden considerar la posibilidad de fortalecer su capacidad para llevar registros de delitos conexos e intercambiar información a nivel regional e internacional acerca de la actividad de grupos delictivos

[237] http://www.un.org/es/events/crimecongress2015/conference-programme.shtml
[238] Naciones Unidas, 13° *Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal,* Doha (Qatar), 2015, p. 3 y 4.

organizados, los *modus operandi* de estos grupos y las técnicas empleadas en la identificación de distintas formas de ciberdelincuencia[239].

Esta recomendación que ofrece la ONU es una de las más importantes para hacer frente a la cibercriminalidad, pues, al intercambiar información con otros organismos del ámbito local (como por ejemplo con las policías cibernéticas de diferentes Estados de la República) e internacional (como lo hace México con Estados Unidos y España, véase la página 122 y 123), fluye la información con el objetivo de conocer la política criminal más adecuada.

2. Los Estados Miembros pueden considerar la posibilidad de garantizar un enfoque jurídico equilibrado que tipifique como delitos específicos los actos básicos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos y, al mismo tiempo revisar la aplicabilidad de otros delitos de carácter general como el robo, el fraude, la falsificación y los daños personales, a los actos cometidos en línea[240].

Como ya referimos en el capítulo segundo de este trabajo de investigación (véase las páginas 81 a la 87), al C.P.F. le faltan muchas disposiciones de delitos que se puedan cometer por medio de la informática, en ese sentido, México aún no ha acatado a esta recomendación de tipificar estas conductas como tales.

3. Los Estados Miembros tal vez necesiten encontrar formas de promover la cooperación internacional en asuntos penales. En la esfera de los delitos cibernéticos, esto puede suponer, en particular, estudiar las posibilidades de agilizar los procedimientos formales de asistencia judicial recíproca y fortalecer la cooperación entre autoridades encargadas de hacer cumplir la ley y mantener un diálogo multilateral continuo sobre el acceso trasnacional a datos informáticos[241].

---

[239] *Ibídem,* pp. 20 y 21.
[240] *Ibídem,* p. 21.
[241] *Idem.*

En ese sentido a esta recomendación, consideramos que la ONU hace referencia a ella, para que los Estados Miembros cooperen entre sí y se compartan mutuamente sus políticas criminales con el objetivo de mejorar la implementada por el Estado.

4. La UNODC debería seguir prestando asistencia técnica a los Estados Miembros con el fin de fortalecer las respuestas de prevención del delito y justicia penal frente a la cibercriminalidad a petición de las organizaciones internacionales pertinentes y en coordinación con ellas[242].

En el 12° Congreso la ONU también hizo esta recomendación, sin embargo, como mencionamos anteriormente, en México no se ha tenido apoyo por parte de la UNODC respecto al ámbito de la cibercriminalidad, lo que consideramos que es importante que se acate a esta recomendación para poder fortalecer la política criminal de México.

5. Los Estados Miembros podrían adoptar un enfoque holístico en relación con la ciberdelincuencia que tenga en cuenta tanto los modus operandi y las amenazas delictivas actuales como su posible evolución futura[243].

Al tener en cuenta un enfoque holístico que adopten tanto la legislación nacional como en el ámbito internacional, ayudaría a unificar los tipos penales, las legislaciones y las políticas criminales, por lo que sería una buena alternativa en el ámbito internacional para hacer frente a la cibercriminalidad.

De este modo, después de haber analizado estos dos congresos, nos damos cuenta que a México le faltan algunas recomendaciones por aplicar a la política criminal que actualmente está operando, por ello, y para mayor claridad, procederemos a analizar la Estrategia Nacional de Ciberseguridad de México.

La Estrategia Nacional de Ciberseguridad (ENCS) es el documento que establece la visión del Estado mexicano en la materia, a partir del

[242] *Ibídem,* p. 22.
[243] *Idem.*

reconocimiento de: A) La importancia de las TIC como factor de desarrollo político, social y económico en México; B) Los riesgos relacionados con el uso de las tecnologías y el creciente número de ciberdelito y; C) La necesidad de una cultura general de ciberseguridad[244].

De este modo, la ENCS es el documento donde se establece parte de la política criminal que planeta México para hacer frente a la cibercriminalidad, dicha estrategia, tiene alcances muy amplios al prever aspectos del sector gubernamental, legislativo, privado y social.

El objetivo general de la ENCS es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político, que permita a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para el desarrollo sostenible del Estado mexicano[245].

La ENCS establece en su objetivo general, como plan de política criminal, es dar a conocer a la sociedad, al sector público y privado el buen uso de las TIC, con el objeto de crear una cultura de civismo digital para la prevención de los ciberdelitos.

En el contexto internacional la ENCS se apoya de la ONU, la Cumbre Mundial de la Sociedad de la Información, el Grupo de Expertos Gubernamentales, la Comisión y Prevención del Delito y Justicia Penal, el Foro para la Gobernanza de Internet, la Unión Internacional de Telecomunicaciones, entre otros más[246].

La ENCS se apoya de una serie de organismos internacionales de España, Estados Unidos, entre otros más, con el objetivo de cooperar internacionalmente con estos mismos, en la lucha de la ciberdelincuencia, intercambiar informaciones tal como lo recomienda la ONU en el 13° Congreso.

---

[244] Gobierno de la República Mexicana, *Estrategia Nacional de Ciberseguridad,* México, 2017, p. 2.
[245] *Ibídem,* p. 4
[246] *Ibídem,* pp. 9-12.

Para lograr el objetivo general, la ENCS, plantea 5 objetivos estratégicos (Sociedad y derechos, Economía e innovación, Instituciones públicas, Seguridad pública, y Seguridad nacional), cuyo desarrollo requiere de 8 ejes transversales (Cultura de ciberseguridad, Desarrollo de capacidades, Coordinación y colaboración, Investigación y desarrollo e innovación en TIC, Estándares y criterios técnicos, Infraestructuras críticas, Marco jurídico y autorregulación y Medición y seguimiento[247].

Como ya mencionamos, la ENCS tiene aspectos bastantes amplios, para cumplirlos, se han establecido estos objetivos y ejes transversales, en ese sentido, lo que se busca es contrarrestar al país de las conductas ilícitas que se desprenden de la informática.

Para llevar a cabo estos 5 objetivos estratégicos, y los 8 ejes transversales, estos mismos, se apoyarán de estrategias implementadas por el Estado mediante el desarrollo de políticas públicas, estrategias, programas, proyectos, acciones e iniciativas, todas estas, para contrarrestar la cibercriminalidad en el país[248].

Cada uno de estos ejes están apoyados por políticas públicas, programas o proyectos; como por ejemplo, para efectuar el eje de cultura de ciberseguridad, se ha implementado por parte de las policías cibernéticas campañas de pláticas informativas para dar a conocer la prevención de ciberdelito, faltará ver que más programas se van a desarrollar para hacer efectivos los demás ejes transversales

En el eje de "Marco jurídico y autorregulación" se contempla la homologación y armonización de los códigos penales complementarias en relación a ciberdelitos, así como las herramientas jurídicas con las que cuentan las instancias de procuración de justicia para la persecución de los mismos[249].

Bajo la lógica de este eje, como política criminal de México, se está adoptando en la ENCS la recomendación número 5 que emitió la ONU en el 13°

[247] *Ibídem,* pp. 17-23.
[248] I*bídem*, pp. 19- 23.
[249] *Ibídem,* pp. 22 y 23.

Congreso, sin embargo, hasta la actualidad no se ha puesto en marcha dicha homologación de leyes en el país, dado que en los estados de la República Mexicana los tipos penales son muy diferentes a otros estados y eso causa que no exista una homologación (véase las páginas 57 a la 60 del segundo capítulo de este trabajo de investigación).

De esta manera, es como México está planeando la política criminal del país para actuar en contra de la cibercriminalidad, en ese sentido, podemos ver que México si ha acatado algunas recomendaciones que ha hecho la ONU en sus Congresos para contrarrestar este delito, sin embargo, como ya referimos anteriormente, aún faltan otras situaciones que faltan seguir para perfeccionar la política criminal del país.

# CONCLUSIONES

De la investigación realizada se infieren ocho conclusiones:

PRIMERA: La mayoría de los Códigos Penales Estatales tipifican el delito de Acceso ilícito a sistemas y equipos informáticos de manera muy diversa al Código Penal Federal, lo que provoca que no exista una homologación o uniformidad legislativa en el país.

SEGUNDA: Son muchos los modus operandi con los que se puede atentar en contra de la información contenida en los sistemas y equipos informáticos, por lo tanto se le deben de dar el tratamiento legislativo necesario a cada uno de ellos.

TERCERA: Algunas conductas que parten de los sistemas informáticos no se encuentran tipificadas por el Código Penal Federal como delitos cometidos por medio de la informática, y ante lo precisa que debe ser la ley penal para sancionar, se requiere que se subsanen estas omisiones legislativas.

CUARTA: La cooperación internacional en materia de los delitos informáticos es fundamental para la prevención de la misma, es por ello que ésta debe de ser la base primordial para que los países logren una unificación y armonía legislativa para contrarrestar a la cibercriminalidad.

QUINTA: Como pudimos apreciar anteriormente al Código Penal Federal le faltan muchas disposiciones con respecto a los delitos informáticos, estas mismas si se encuentran reguladas por las legislaciones de Alemania, Francia y España, bajo esa lógica, inferimos que para brindar mayor certeza jurídica a la ley se deben de contemplar esas disposiciones en el Código Penal Federal para evitar el rezago legislativo de estas conductas ilícitas en el país.

SEXTA: Para luchar en contra de la cibercriminalidad se necesita que todos los países cooperen con la INTERPOL y que en estos mismos se establezcan policías cibernéticas que actúen en su territorio, para hacer ágil la investigación de este tipo de delito y evitar impunidades.

SEPTIMA: En el aspecto de la política criminal en materia de los delitos informáticos, es de suma importancia que los países tomen en cuenta las recomendaciones que emite la ONU con el objetivo de tomar medidas para la prevención de este delito.

OCTAVA: Aunque México ya ha acogido algunas recomendaciones hechas por la ONU en la ENCS, aún le falta ponerlas en marcha, como por ejemplo, la referida en la conclusión primera, por lo tanto se debería de cumplir con el objetivo de que esta recomendación no se quede en letra muerta aparte de que el país lo requiere.

## PROPUESTA

No cabe duda que las conductas antijurídicas desprendidas de la informática y la Internet son relativamente nuevas, por lo tanto, la ley que las regula debe de estar al día con los actos que van surgiendo actualmente y regularlos en el cuerpo jurídico que las conforma.

Asimismo, como se analizó en el capítulo segundo del presente trabajo de investigación, el delito de acceso ilícito a sistemas y equipos de informática comprende una amplia gama de modalidades con las que puede ser comisionado, como los son: el acceso ilícito; espionaje informático; sabotaje informático; virus informático; gusanos informáticos; bombas lógicas o cronológicas; caballo de Troya; manipulación informática; robo de información; piratería informática; *hacking* y *cracking*.

Por ello, ante las variadas conductas con las que se puede realizar este delito, es que proponemos que estas sean tipificadas de forma más clara y precisa en el Capítulo II denominado "Acceso ilícito a sistemas y equipos de informática" correspondiente al Título noveno "Revelación de secretos y acceso ilícito a sistemas y equipos de informática" del Código Penal Federal, con el objetivo que se le dé el tratamiento adecuado a cada una de ellas, evitar omisiones legislativas y vacíos legislativos para que a su vez la ley penal no tenga atipicidades.

Con dicha reforma, estaríamos a la par con países como Alemania, Francia y España, quienes contemplan supuestos de hechos no regulados por el Código Penal Federal como: determinar la utilización ilícita de los datos informáticos obtenidos; obstaculizar o interrumpir el funcionamiento de los sistemas informáticos en general no sólo aquellos que pertenezcan a la impartición de justicia; así como también el acto de permanecer en el sistema informático

De la misma forma, de la Internet y de la informática se comisionan otros delitos diferentes al delito de Acceso ilícito a sistemas y equipos de informática, como los son: el fraude informático; la usurpación de identidad y el *ciberbullyng* o el ciberacoso. En ese sentido, el fraude informático afecta el bien jurídico del

patrimonio económico, y la usurpación de identidad por medios informáticos (robo de identidad) también afecta el patrimonio económico pero también se afecta a la propia persona en su dignidad; mientras que el ciberbullyng o el ciberacoso afecta al bien jurídico de la paz y la seguridad de las personas.

De esta manera, las anteriores conductas ilícitas no se encuentran reguladas por el Código Penal Federal, así que se encuentran sin tipificación alguna, por lo cual, proponemos que también sean incorporadas a dicho ordenamiento jurídico, en los respectivos títulos y capítulos que les corresponden, debido a la afectación que estas mismas tienen.

En esa importancia, se tienen que establecer leyes que especifiquen de forma clara y precisa las prácticas ilícitas ocurridas por medio de la web y la informática, debido a que la tecnología se va innovando constantemente y a la vez estas conductas ilícitas también se van perfeccionando, por lo que no podemos tener leyes rezagadas que no contemplen los eventos actuales.

Por otra parte, en el campo de la investigación de este tipo de delito, las policías cibernéticas son de reciente creación en México, algunos estados ya las tienen en su función, y en otros apenas se están instalando (tal como lo vimos en el tercer capítulo).

Por lo que proponemos, que en todas las entidades federativas se establezcan policías cibernéticas que actúen en contra de los ciberdelitos, especialmente en el estado de Sinaloa en donde el H. Congreso del Estado rechazó la propuesta de establecer una policía cibernética del ámbito local, y ante la falta de este organismo especializado en informática los ciberdelitos seguirán en aumento.

PROPUESTA LEGISLATIVA

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPÍTULO II

Acceso ilícito a sistemas y equipos de informática

*Artículo 211 bis 1.- Al que sin autorización acceda a datos de un sistema o equipo de informática no destinados a él, y que estén protegidos contra accesos no autorizados superando la seguridad de acceso que proporciona, se le impondrá de seis meses a un año de prisión.*

*Al que por cualquier medio o procedimiento, vulnerando las medidas de seguridad facilite a otro el acceso al conjunto, o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho de excluirlo, será castigado con una pena de prisión de seis meses a dos años de prisión.*

Artículo 211 bis 2.- Al que sin autorización modifique, *provoque la inutilización***,** destruya o provoque perdida de información contenida en sistemas o equipos de informática, protegidos por algún mecanismo de seguridad, se le impondrá de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca, *obtenga,* copie *o utilice* información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

*Artículo 211 bis 3.- Al que sin la autorización permanezca en todo o en una parte de un equipo o sistema informático, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

*Artículo 211 bis 4.- El que sin estar autorizado y de manera grave obstaculizara, interrumpiera o interfiriera en el funcionamiento de un sistema informático ajeno, se le impondrán de seis meses a tres años de prisión.*

*Artículo 211 bis 5.- El que produzca, adquiera para su uso, importe o facilite a terceros una un programa informático, contraseña o un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información, se le impondrá de seis meses a dos años de prisión y de cien a trescientos días multa.*

*Artículo 211 bis 6.- Si el responsable es o hubiera sido la persona encargada del equipo o sistema informático, se le impondrá de uno a cuatro años de prisión.*

*Artículo 211 bis 7.- Al que sin estar autorizado se apodere, utilice o modifique en perjuicio de un tercero datos electrónicos de carácter personal o familiar de otro o se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro archivo o registro público o privado, se le impondrá de un año a cuatro años de prisión y de ciento cincuenta a cuatrocientos días multa.*

*Se impondrá la pena de prisión de dos a cinco años de prisión si dichos datos informáticos se difunden, revelan o ceden a terceros.*

Artículo 211 bis 8.- Al que sin autorización modifique, *provoque la inutilización,* destruya, o provoque perdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca, *obtenga,* copie o *utilice* información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegidos por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se le impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia,

o recaiga sobre los registros relacionados con el procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 9.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, *provoque la inutilización,* destruya o provoque perdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente *obtenga,* copie o *utilice* información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se le impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Artículo 211 bis 10.- Al que sin autorización modifique, *provoque la inutilización,* destruya, o provoque perdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sector financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca, *obtenga,* copie o *utilice* información contenida en sistemas o equipos de informática de las instituciones que integran el sector financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Artículo 211 bis 11.- A quien estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sector financiero,

indebidamente modifique *provoque la inutilización,* destruya, o provoque perdida de información que contenga, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sector financiero, indebidamente *obtenga*, copie o *utilice* información que contengan, se le impondrá de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sector financiero.

Artículo 211 bis 12.- Para los efectos de los artículos *211 Bis 4 y 211 Bis 5* anteriores, se entiende que por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Artículo 211 bis 13.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se altere o utilice en perjuicio del titular de los datos electrónicos en provecho propio de un tercero.

TÍTULO VIGESIMO SEGUNDO

Delitos en contra de las personas y su patrimonio

CAPÍTULO III

Fraude

Artículo 387.- Las mismas penas señaladas en el artículo anterior se impondrán:

*Fracción XXII.- Al que se dé a sí mismo o a un tercero una ventaja financiera ilegal, introduciendo fraudulentamente datos en un sistema de procesamiento automatizado, diseñando ilícitamente un programa informático, o manipulando una base de datos mediante la utilización de datos incorrectos o incompletos a través del uso no autorizado de datos.*

*Fracción XXIII.- Al que por medios informáticos obtenga información de carácter personal de un individuo tal como la información identificable, financiera, o médica y que esta misma sea utilizada en provecho propio o ajeno para un tercero, haciéndose pasar como el dueño de dichos datos con el objeto de tener una ventaja financiera ilegal.*

## TITULO DÉCIMO OCTAVO

## Delitos en contra de la paz y la seguridad de las personas

### CAÍTULO I

### Amenazas y cobranza extrajudicial

Artículo 282.- se aplicará sanción de tres días a un año de prisión o de ciento ochenta a trescientos sesenta días multa:

*Fracción III.- Al que por medios informáticos, telemáticos o electrónicos amenace a otro con causarle mal en su persona, en sus bienes, en su honor o en sus derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado a un vínculo.*

*Fracción IV.- Al que por medios informáticos amenace, acose, atormente, humille o avergüence a una persona.*

## GLOSARIO DE SIGLAS

ARPANET: *Avanced Research Projet Agency Network, "*Agencia de Proyectos de Investigación Avanzada

CERN: *Conseil Européen pour la Recherche Nucleaire, "*Consejo de Investigadores Europeos

CSNET: *The Computer Sciencie Network "*Red de Ciencias de la Computación"

C.P.F: Código Penal Federal

ENCS: Estrategia Nacional de Ciberseguridad

FTC: *Federal Trade Commission*, "Comisión Federal de Comercio"

INEGI: Instituto Nacional de Estadística y Geografía

INTERPOL: Organización Internacional de Policía Criminal

IBM: *International Business Machines Corporation*

MILNET: *Military Network* "Red Militar"

NSFNET: *National Science Fundation Network* "Fundación Nacional para la Ciencia"

UNODC: Oficina de las Naciones Unidas Contra la Droga y el Delito

OCDE: Organización para la Cooperación y Desarrollo Económico

ONU: Organización de las Naciones Unidas

STC: Secretaría de Comunicaciones y Transporte

TIC: Tecnologías de la Información y la Comunicación

WI-FI: *Wireless Fidelity* "Fidelidad sin cables o inalámbrica"

WWW: *World Wide Web "*Red informática Mundial"

# FUENTES CONSULTADAS

## BIBLIOGRÁFICAS


ABELEDO DÍAZ, Miguel Ángel, *Aspectos legales de los negocios online,* España, Wolters Kluwer, 2012

ABOSO, Gustavo Eduardo, *Derecho penal cibernético,* Argentina, euros editores, 2017

ABOSO, Gustavo Eduardo y ZAPATA, María Florencia, *Cibercriminalidad y derecho penal*, Argentina, Editorial B de F, 2006

ÁGUILA, Ana Rosa del, *Comercio electrónico y estrategia empresarial: Hacia la economía digital,* 2a ed., España, Alfaomega Grupo Editor, 2001

ALMENAR PINEDA, Francisco, *El delito de hacking,* España, Editorial Arizandi, 2018

ANTOLISEI, Francesco, *Manual de derecho penal,* 8a. ed., trad. Jorge Guerrero y Marino Ayerra Redín, Colombia, 1988

ATIENZA, Manuel, *El sentido del derecho,* España, Ariel editores, 2001

AZAOLA CALDERÓN, Luis, *Delitos informáticos y derecho penal,* México, Ubijus Editorial, 2010

BALMACEDA HOYOS, Gustavo, *El delito de estafa informática,* Colombia, Leyer Editorial, 2009

CÁMPOLI, Gabriel Andrés, *Derecho penal informático en México,* México, Instituto Nacional de Ciencias Penales, 2004

CARBALLAR, José A., *Wi-Fi instalación, seguridad y aplicaciones,* México, Alfaomega Grupo Editor, 2007

CARDEÑO SHAADI, José Ramón, *Las patentes de software,* México, Porrúa, 2013

CARRANCA Y TRUJILLO, Raúl, *Derecho penal mexicano parte general,* 15a ed., México, Porrúa, 1986

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

CRUZ DE PABLO, José Antonio, *Derecho penal y nuevas tecnologías. Aspectos sustantivos,* España, Grupo Difusión jurídica y temas de actualidad, 2006

DÍAZ REVORIO, Francisco Javier, *Los derechos humanos ante los nuevos avances científicos y tecnológicos,* México-España, Tirant Lo Blanch, 2009

DUPUY, Daniela (Dir.), *Cibercrimen,* Argentina, Euros editores, 2016

DURÁN DÍAZ, Oscar Jorge (coord.), *Derecho y medios electrónicos, temas selectos,* México, Porrúa, 2012

ESCUDERO GALLEGO, Román y MARTÍNEZ GARRIDO, Santiago (Dirs.), *Cuadernos de derecho para ingenieros, ciberseguridad,* España, Wolters Kluwer España, 2017

ESTABROOK, Noel y BILL, Vernon, *Aprendiendo internet en 24 horas*, trad. de Ricardo de la Barrera Ugalde, Estados Unidos, Prentice-Hall Hispanoamericana, 1997

FERNÁNDEZ RODRÍGUEZ, José Julio, *Lo público y lo privado en internet, intimidad y libertad de expresión en la red*, México, UNAM, Instituto de investigaciones jurídicas, 2004

FERNÁNDEZ RODRÍGUEZ, José Julio y SANSÓ- RUBERT PASCUAL, Daniel (eds.), *Internet: un nuevo horizonte para la seguridad y defensa,* España, Universidad de Santiago de Compostela, 2010

FERREYRA CORTÉS, Gonzalo, *Informática para cursos de bachillerato,* México, Alfaomega Grupo Editor, 2000

FLORES SALGADO, Lucerito, *Derecho informático,* México, Editorial Patria, 2009

GALÁN MUÑOZ, Alfonso, *El fraude y la estafa mediante sistemas informáticos análisis del artículo 248.2 del C.P.,* España, Tirant lo Blanch, 2005

GARCÍA GONZÁLEZ, Javier (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant Lo Blanch, España, 2010

GARCÍA MEXIA, Pablo (coord.), *Principios de derecho de Internet,* España, Tirant lo Blanch, 2002

GARCÍA RAMÍREZ, Sergio y GONZÁLEZ MARISCAL DE, Olga Islas (comps.), *Derecho penal y criminalística XII jornadas sobre justicia penal,* México, UNAM, Instituto de Investigaciones Jurídicas, Instituto de la Formación de la Procuraduría General de Justicia del Distrito Federal, 2012

GARRIGA DOMÍNGUEZ, Ana (coord.) Fundamentos éticos y jurídicos de las TIC, España, Editorial Aranzadi, 2012

GÓMEZ VEITETES, Álvaro, *Enciclopedia de la seguridad informática*, México, Alfaomega grupo editor, 2007

GONZÁLEZ-SALAS CAMPOS, Raúl, *La teoría del bien jurídico en el derecho penal,* 2a. ed., México, Oxford, 2001

HAHN, Harley, *Internet manual de referencia*, 2a ed., trad. de José Pieltain Álvarez Arenas, España, McGraw-Hill de España, 1997

HERNÁNDEZ CAMARGO, Emiliano, *La informática jurídica y legislativa en México,* México, Consejo Nacional de Ciencia y Tecnología

HIDALGO BANILLA, Antonio, *Derecho informático,* México, Flores editor y distribuidor, 2013

HOCSMAN, Heriberto Simón, *Negocios en Internet,* Colombia, Editorial Astreas, 2013

HUIDOBRO MOYA, José Manuel y MILLÁN TEJEDOR, Ramón Jesús, *Redes de datos y convergencia IP*, México, Alfaomega Grupo Editor, 2008

IVENS, Kathy, *Internet en casa,* trad. de Luiciano García Tosina, España, McGraw-Hill Interamericana de España, 2004

J. MAILER, Julio B. (coord.), *Delitos no convencionales,* Argentina, Editores del Puerto, 1994

JIMÉNEZ DE ASÚA, Luis, Lecciones de derecho pena, México, Oxford University Press, 1999, v III

JIMÉNEZ HUERTA, Mariano*, Derecho penal mexicano,* 2a ed., México, Porrúa, 1977, t. I

JOYANES, Luis, *Cibersociedad los retos sociales ante un nuevo mundo digital*, España, McGraw-Hill/ interamericana de España, 1997

KENT, Peter, *Serie ¡fácil! Internet*, 3a. ed., trad. Miguel Morales Carbajal, México, Prentice Hall Hispanoamericana, 1998

LAN ARREDONDO, Arturo Jaime, *Sistemas jurídicos,* México, Oxford, 2011

LÓPEZ ANGULO, Tania Clarisa et al., *Laboratorio de computo II,* 2a ed., México, Universidad Autónoma de Sinaloa, 2009

LÓPEZ CALVO, Pedro, *Derechos humanos, victimología, terrorismo y sus diversas modalidades delictivas, secuestros, delitos informáticos y armas de destrucción masiva,* México, editorial Flores, 2015

LUQUE ORDOÑEZ, Javier, *Videoconferencia tecnología, sistemas y aplicaciones,* México, Alfaomega Grupo Editor, 2009

LUZ CLARA, Bibiana, *Manual de derecho informático*, Argentina, Editorial jurídica Nova Tesis, 2001

MALO CAMACHO, Gustavo, *Derecho penal mexicano,* 7a. ed., México, Porrúa, 2013

MARÍN PEIDRO, Lucia, *Los contenidos ilícitos y nocivos en Internet,* España, Fundación Retevisión, 2000

MARQUINA SÁNCHEZ, María de Lourdes, *Gobernanza global del comercio en internet,* México, Instituto Nacional de Administración pública, 2012

MATA BARRANCO DE LA (Coord.), *Derecho penal informático,* España, Editorial Aranzadi, 2010

MAYER, Max Ernst, *Derecho penal parte general,* trad. Sergio Politoff Lifschitz, Argentina, editorial B de F, 2007

MEDINA ORTEGA, Cutberto Simón, *Contabilidad financiera jurídica y fiscal*, 2a ed., México, 7 editores, 2012

MENÉNDEZ MATO, Juan Carlos y GAYO SANTA CECILIA, Ma. Eugenia, Derecho e informática. Ética y legislación, España, Bosch Editor, 2014

MEZGER, Edmund, *Derecho penal parte general,* 2a. ed., México, Cárdenas Editor y Distribuidor, 1990

MIGUEL MOLINA DE, María del Rosario y Oltra Gutiérrez, Juan Vicente, *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas,* España, Editorial de la UPV, 2007

MOLINA SALGADO, Jesús Antonio, *Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial,* México, Porrúa, 2003

MONTOYA PIÑA, Javier Omar, *Delitos federales cometidos a través de medios informáticos,* México, Flores editor, 2015´

MUÑOZ CONDE, *Derecho penal parte especial,* 14 a ed., España, Tirant Lo Blanch, 2002

NAVA GARCÉS, Alberto Enrique, *Análisis de los delitos informáticos,* 2a. ed., México, Porrúa, 2007

NAVA GARCÉS, Alberto Enrique (coord.), *El derecho en la era digital,* México, Porrúa, 2013

NORTON, Peter, *Introducción a la computación,* 6a. ed., México, McGraw-Hill/Interamericana Editores, 2006

PALAZZI, Pablo Andrés, *Delitos informáticos,* Argentina, AD-HOC editores, 2000

PALOMA PARRA, Luis Orlando, *Delitos informáticos (en el ciberespacio),* Colombia, Ediciones jurídicas Andrés Morales, 2012

PARDINI, Anibal A., *Derecho de internet,* Argentina, Ediciones La Roca, 2002

PAVÓN VASCONCELOS, *Manual de derecho penal mexicano,* 16a. ed., México, Porrúa, 2002

PEÑA TRESANCOS, Jaime y Vidal Fernández, María Carmen, *Introducción a la informática*, España, McGraw-Hill/Interamericana de España, 2004

REGIS PRADO, Luiz, *Bien jurídico y constitución,* trad. de Luis Enrique Álvarez Aranda, Perú, Ara editores, 2010

RIVAS MAYETT, Diana, *Cibercriminalidad en México,* México, Servicio express de impresión, 2012

ROJAS AMANDI, Víctor, *El uso de internet en el derecho*, 2a. ed., México, Oxford, 2009

ROMEO CASABONA, Carlos María (coord.), *El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Editorial Colmares, España, 2006

ROMERO LÓPEZ, Lucero (coord.), *Jus informa TIC´s,* México, s.e., 2011

RUELAS, Ana Luz, *Internet y los accesos públicos: cibercafés en Sinaloa,* México, Universidad Autónoma de Sinaloa, 2012

SÁEZ CAPEL, José, *Informática y delito,* 2a. ed., Argentina, Proa XXI editores, 2001

SAIN, Gustavo Raúl, *Delito y nuevas tecnologías,* Argentina, Editores del Puerto, 2012

SALOM CLOTET, Juan, "Delito informático y su investigación", *Delitos en contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, España Consejo General del Poder Judicial, 2006

SÁNCHEZ MONTÚFAR, Luis, *Informática,* México, Pearson Educación, 2005

SANCHIS CRESPO, Carolina (coord.), *Fraude electrónico: entidades financieras y usuarios de banca,* Editorial Aranzadi, España, 2011

SANCHIS CRESPO, Carolina (coord.), *Fraude electrónico, panorámica actual y medios jurídicos para combatirlo*, Editorial Aranzadi, España, 2013

TÉLLEZ CARVAJAL, Evelyn (coord.), *Derecho y TIC. Vertientes actuales,* México, UNAM, Instituto de Investigaciones Jurídicas, 2016

TÉLLEZ VALDÉS, Julio, *Derecho informático,* 4a ed., México, McGraw-Hill Interamericana, 2009

VÁZQUEZ-PORTOMEÑE SEIJAS, Fernando (Dir.), *Estudios penales criminológicos XXIX*, España, Universidad de Santiago de Compostela, 2009

VELASCO NUÑEZ, Eloy, *Delitos cometidos a través de internet. Cuestiones procesales*, España, La ley grupo Wolters Kluwer España, 2010

VILLAREAL DE ANAYA, Sonia, *Introducción a la computación: guía práctica para el aprendizaje de paquetes,* México, McGraw-Hill Interamericana Editores, 1999

HEMEROGRAFÍA

ÁVILA PIETRASANTA, Irma, "*Internet: espacio de ejercicio de derechos para niños",* Revista Zócalo, México, Año XV, Número 185, Julio 2015

CENTRO DE INVESTIGACIÓN DE LA WEB, *Cómo funciona la web,* Chile, Universidad de Chile, 2008

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS, *Avances tecnológicos de los Derechos Humanos, fascículo 4,* México, Comisión Nacional de los Derechos Humanos, 2004

ESTEBAN NAVARRO, Miguel Ángel, *"Los archivos de documentos electrónicos",* El profesional de la información, España, Vol. 10, Número 12, Diciembre de 2001.

GOBIERNO DE LA REPÚBLICA MEXICANA, *Estrategia Nacional de Ciberseguridad,* México, 2017

GONZÁLEZ HURTADO, Jorge Alexandre, "La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española", *Revista Penal México,* México, 2016, Número 9, Septiembre de 2015- enero 2016

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA INEGI, *Encuesta Nacional Sobre la Disponibilidad y Uso de las TIC en los Hogares 2018 (ENDUTIH 2018),* México, abril 2019

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA INEGI, *Estadística a propósito del día mundial del internet*, México, mayo de 2017

NACIONES UNIDAS, *12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal,* Salvador (Brasil), 2010

NACIONES UNIDAS, 13° *Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal,* Doha (Qatar), 2015

## LEYES CONSULTADAS

CÓDIGO PENAL FEDERAL (vigente de última reforma publicada en el Diario Oficial de la Federación del 12 de abril de 2019)

CÓDIGO PENAL DE ALEMANIA (Versión del año 2013)

CÓDIGO PENAL DE ESPAÑA (Última actualización de 23 de noviembre de 2016)

CÓDIGO PENAL DE FRANCIA (Versión consolidada del año 2014)

CÓDIGO PENAL PARA EL ESTADO AGUASCALIENTES (última reforma publicada en el Periódico Oficial de fecha del 7 de noviembre de 2016)

CÓDIGO PENAL PARA EL ESTADO BAJA CALIFORNIA (última reforma publicada en el Periódico Oficial Numero 34, Sección 1 de fecha del 18 de julio de 2017)

CÓDIGO PENAL PARA EL ESTADO DE CHIAPAS (última reforma publicada en el Periódico Oficial Numero 315 segunda sección de fecha del 20 de agosto de 2017)

CÓDIGO PENAL PARA EL ESTADO DE CAMPECHE (última reforma publicada en el Periódico Oficial Numero 315 segunda sección de fecha del 20 de agosto de 2017)

CÓDIGO PENAL PARA EL ESTADO DE CHIHUAHUA (última reforma publicada en el Periódico Oficial Número 86 de fecha del 28 de octubre de 2017)

CÓDIGO PENAL PARA EL ESTADO DE COAHUILA DE ZARAGOZA (última reforma publicada en el Periódico Oficial de fecha del 06 de octubre de 2017)

CÓDIGO PENAL PARA EL ESTADO DE COLIMA (última reforma por decreto 183 de fecha del 10 de diciembre de 2016)

CÓDIGO PENAL PARA EL ESTADO DE HIDALGO (última reforma publicada en el Periódico Oficial del Estado el 09 de octubre de 2017)

CÓDIGO PENAL PARA EL ESTADO DE MÉXICO (última reforma publicada en la Gaceta del Gobierno el 01 de septiembre de 2017)

CÓDIGO PENAL PARA EL ESTADO DE MICHOACÁN DE OCAMPO (última reforma publicada en el Periódico Oficial del Estado el 19 de agosto de 2017)

CÓDIGO PENAL PARA EL ESTADO DE MORELOS (última reforma publicada de fecha de 19 de septiembre de 2017)

CÓDIGO PENAL PARA EL ESTADO DE NAYARIT (última reforma publicada en el Periódico Oficial del Estado el 28 de marzo de 2017)

CÓDIGO PENAL PARA EL ESTADO DE NUEVO LEÓN (última reforma publicada en el Periódico Oficial de 27 de junio de 2017)

CÓDIGO PENAL PARA EL ESTADO QUERÉTARO (última reforma publicada el 01 de septiembre de 2017)

CÓDIGO PENAL PARA EL ESTADO SAN LUIS POTOSÍ (última reforma publicada en el Periódico Oficial de 27 de mayo de 2017)

CÓDIGO PENAL PARA EL ESTADO DE SINALOA (última reforma publicada en el Periódico Oficial número 065 del 24 de mayo de 2017)

CÓDIGO PENAL PARA EL ESTADO SONORA (última reforma publicada en el Boletín Oficial número 10, sección III de fecha 03 de agosto de 2017)

CÓDIGO PENAL PARA EL ESTADO TABASCO (última reforma mediante decreto 112 de fecha 16 de agosto de 2017, publicado en el Periódico Oficial del Estado número 7822 suplemento "B")

CÓDIGO PENAL PARA EL ESTADO TAMAULIPAS (última reforma aplicada en el Periódico Oficial de fecha de 08 de junio de 2017)

CÓDIGO PENAL PARA EL ESTADO YUCATÁN (última reforma publicada en el Diario Oficial de 18 de julio de 2017)

CÓDIGO PENAL PARA EL ESTADO DE ZACATECAS (última reforma publicada en el P. O. G. del 01 de junio de 2016)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE BAJA CALIFORNIA SUR (última reforma por Decreto 193, publicada en el Periódico Oficial de fecha del 13 de julio de 2017)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE DURANGO (última reforma publicada en el Periódico Oficial Numero 19 de fecha de 05 de marzo de 2015)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE GUANAJUATO (última reforma publicada en el Periódico Oficial del Gobierno del Estado Número 180, segunda parte de fecha de 19 de octubre de 2017)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE GUERRERO, Numero 499 (última reforma publicada en el Periódico Oficial del Gobierno del Estado Numero 104 Alcance VII de fecha de 27 de diciembre de 2016)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE JALISCO

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE OAXACA (última reforma publicada en el Periódico Oficial Extra de 1 de mayo de 2017)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE PUEBLA (última reforma publicada el 31 de marzo de 2017)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE QUINTANA Roo (última reforma publicada en el Periódico Oficial del Estado del 19 de julio de 2017)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE TLAXCALA (última reforma publicada en el Periódico Oficial del Gobierno del Estado el 19 de mayo de 2016)

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE VERACRUZ DE LA LLAVE (última reforma publicada en la Gaceta Oficial de 15 de agosto de 2017)

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

DIARIO OFICIAL DE LA FEDERACIÓN, tomo DXLVIII, Número 10, de fecha lunes 17 de mayo de 1999

DIARIO OFICIAL DE LA FEDERACIÓN, tomo DCLXIX, Número 18, de fecha miércoles 24 de junio de 2009

DIARIO OFICIAL DE LA FEDERACIÓN, tomo DCCLIII, número 15 de fecha viernes 17 de junio de 2016

EXPOSICIÓN DE MOTIVOS, Cámara de origen: senadores, de fecha 13 de noviembre de 1999

EXPOSICIÓN DE MOTIVOS, Cámara de origen: diputados, de fecha 02 de octubre de 2009

EXPOSICIÓN DE MOTIVOS, Cámara de diputados, de fecha 09 de diciembre de 2014

PERIÓDICO OFICIAL DEL ESTADO DE SINALOA, Decreto número 539, de fecha 28 de octubre de 1992

SITIOS WEB

DICCIONARIO DE LA LENGUA ESPAÑOLA, http://dle.rae.es/?id=7OpEEFy, consultado el 10 de octubre de 2017

http://congresosanluis.gob.mx/content/atenci%C3%B3ndelitoscibern%C3%A9ticos-por-autoridades-especializadas

http://data.ssp.cdmx.gob.mx/documentos/ciberdelincuencia/infografias/48_Infografia.pdf

http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

https://dle.rae.es/?id=C2rVUUs

https://fge.jalisco.gob.mx/policia-cibernetica

http://s-seguridad.hidalgo.gob.mx/?p=4037

https://sipse.com/novedades/reclutamiento-elementos-aspirantes-policia-cibernatica-analisis-capacitacion-requisitos-examen-cancun-290372.html

http://sseguridad.edomex.gob.mx/seguridad-publica-transito/policia-cibernetica

http://sspsonora.gob.mx/index.php/encuesta-de-satisfaccion-ciudadana/85-destacadas/512-se-prepara-sonora-para-contar-con-division-de-policia-cibernetica.html

http://fiscalia.chihuahua.gob.mx/inicio/?page_id=468

http://nnc.mx/articulo/Policiaca/detenido-por-amenazar-en-facebook-de-una-masacre-en-la-prepa-1/1486657578

http://ntrzacatecas.com/2017/01/20/sin-precisar-creacion-de-policia-cibernetica/

http://uadcgro.blogspot.mx/p/denuncias.html

https://www.20minutos.com.mx/noticia/329809/0/policia-de-baja-california-tiene-nueva-unidad-cibernetica/

http://www.cesmorelos.gob.mx/?page_id=7619

http://www.colimaestado.gob.mx/2016/index.php/portal/noticia/6760017269251293761

https://www.debate.com.mx/culiacan/Sin-recurso-para-Policia-Cibernetica-diputados-20170630-0049.html

http://www.delitosinformaticos.mx/que-es-un-delito-informatico/como-denunciar-delitos-ciberneticos-en-mexico/

http://www.e-tlaxcala.mx/nota/2017-05-28/gobierno/quedo-creada-la-division-cientifica-y-unidad-de-policia-cibernetica-en

https://www.elsiglodetorreon.com.mx/noticia/1348366.unidad-cibernetica-inicia-operaciones.html

http://www.eluniversalqueretaro.mx/portada/01-07-2014/logros-de-policiacibrnetica

https://www.facebook.com/PoliciaCiberneticaGto/

http://www.fiscaliatabasco.gob.mx/Contenido/UnidadDelitosInformaticos

http://www.fge.yucatan.gob.mx/rt.php?seccion=comunicacionsocial&subseccion=noticias&accion=detalles&id=1400&titulo=polic&iacutea-cibern&eacutetica-de-la-fge-llama-a-usar-herramientas-de-privacidad

https://www.interpol.int/es/Crime-areas/Cybercrime/Cybercrime

http://www.milenio.com/policia/diez-agentes-integran-policia-cibernetica-coahuila

http://www.milenio.com/policia/entra-en-operacion-policia-cibernetica

http://www.milenio.com/policia/tendra-nl-ciber-policias

http://www.nuestravision.com.mx/index.php/component/videoflow/play/65233-crean-unidad-de-policia-cibernetica-en-michoacan

http://www.pgjebcs.gob.mx/cibernetica/

http://www.ssp.campeche.gob.mx/index.php/historico-boletines/345-20-02-2018-alerta-policia-cibernetica

https://www.sspc.chiapas.gob.mx/noticias/vgwXuLiUSoc-3D-

http://ssp.puebla.gob.mx/index.php/delitos-ciberneticos

http://www.veracruz.gob.mx/seguridad/atiende-policia-cientifica-casi-300-casos-de-delitos-ciberneticos/

http://www.un.org/es/conf/crimecongress2010/

http://www.un.org/es/events/crimecongress2015/about.shtml

http://www.un.org/es/events/crimecongress2015/conference-programme.shtml

https://www.un.org/securitycouncil/es/content/countries-never-elected-members-security-council

https://www.unotv.com/noticias/estados/aguascalientes/detalle/ya-construyen-cuartel-para-la-ciberpolicia-en-aguascalientes-525001/

https://diario.mx/noticias/television/programas-de-noticias/primer-policia-cibernetica-en-oaxaca/

SECRETARÍA DE COMUNICACIONES Y TRANSPORTES, Lineamientos del proyecto México conectado, México, 2013, *http://mexicoconectado.gob.mx/images/archivos/2013_09_27_Lineamientos_Mexico_Conectado.pd*