ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALÍA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PÚBLICA

T E S I N A

"LOS DELITOS INFORMÁTICOS Y SUS VARIANTES EN EL SISTEMA PENAL MEXICANO Y SU REGULACIÓN."

Para obtener el Grado de

MAESTRA EN GESTIÓN DE SISTEMAS DE SEGURIDAD PÚBLICA.

Catedrática: MTRA. ETHEL GARZA ARMENDÁRIZ

Postulante: LIC. DIANA CRISTINA HEIRAS RAMOS

Chihuahua, Chih. A 13 de junio de 2022

FISCALÍA GENERAL DEL ESTADO

ESTADO LIBRE Y SOBERANO DE CHIHUAHUA

Secretaría de Educación y Deporte

FISCALÍA GENERAL DEL ESTADO

INSTITUTO ESTATAL DE SEGURIDAD PÚBLICA

T E S I N A

"LOS DELITOS INFORMÁTICOS Y SUS VARIANTES EN EL SISTEMA PENAL MEXICANO Y SU REGULACIÓN."

Para obtener el Grado de:

MAESTRA EN GESTIÓN DE SISTEMAS DE SEGURIDAD PÚBLICA.

Catedrática: MTRA. ETHEL GARZA ARMENDÁRIZ

Postulante: LIC. DIANA CRISTINA HEIRAS RAMOS

Chihuahua, Chih. A 13 de junio de 2022

AGRADECIMIENTO

De manera muy especial y sincera a la persona que me guio en este reto, que fue el desarrollo de la presente tesina a la Mtra. Ethel Garza Armendáriz a quien debo destacar su disponibilidad y paciencia, no cabe duda que su preparación ha enriquecido el trabajo realizado.

Quiero expresar también un fuerte agradecimiento a este honorable Instituto Estatal de Seguridad Publica, que se ha dedicado a formar profesionistas con verdadera vocación de procuración de justicia.

DEDICATORIA

A mis padres Jesús e Imelda, que me han dado todo lo que soy como persona, mis valores y mis principios los cuales me han permitido llegar a cumplir un sueño más, gracias por inculcar en mí el esfuerzo y darme la valentía para no temer a las adversidades, este logro no sería nada sin ustedes.

A mis hermanos Adriana, Gabriela y Jesús, las personas que sin importar nuestras diferencias siempre me han apoyado de forma incondicional.

A mi esposo Víctor Hugo, el hombre que siempre me ha impulsado a vencer miedos y convertirlos en fortalezas, que me enseño destrezas y habilidades que jamás pensé, existieran en mí, a quien cada día amo y admiro más.

A mis amigo y colegas, por permitirme aprender más de la vida con sus experiencias.

INTRODUCCIÓN

Dentro de la legislación en México no existe como tal la clasificación legal de los delitos informáticos; dentro del Código Penal Federal o ya sea de carácter estatal no se localiza Capítulo o un delito con tal denominación.

Sin embargo, existen algunas conductas ilícitas que pueden llegar encuadrarse en el tipo penal que a lo largo del presente trabajo se identifican y podrían ser parte de los denominados delitos Informáticos y/o delitos cibernéticos ya que se encuentran previstas y sancionadas en los Códigos Penales de las Entidades Federativas y posteriormente las que se prevén en la legislación penal federal.

Con la llegada de la era digital el día a día de la sociedad ha cambiado radicalmente y con ello la comisión de delitos por medios informáticos, dando un gran desafío a las instituciones de procuración de justicia de México, por lo que algunas de estas instituciones han contemplado en sus legislaciones áreas específicas encargadas de dar el seguimiento pertinente a este tipo de conductas delictivas que tienen como fin vulneran los derechos fundamentales de los usuarios.

ÍNDICE

CAPÍTULO PRIMERO

CONCEPTUALIZACIÓN DEL DESARROLLO DEL TEMA

Sabemos que el año 2020 quedará marcado como el año donde el mundo se enfrentó a una de las más grandes pandemias en la historia y con esto, a un cambio en el modo de vida de las personas.

Este cambio tuvo como elemento central el uso de las tecnologías de la información a nuestro alrededor. Si bien, el uso de nuevas tecnologías evolucionaba rápidamente, aún existían muchos sectores de la población que no las integraban por completo. Con la llegada de la pandemia, el mundo tuvo la necesidad de adaptarse a una nueva forma de interactuar, desde la forma de convivir con la familia, el estilo de trabajar, el modo de adquirir productos, la forma impartir y tomar clases, entre otras actividades. La pandemia que estaba iniciando ocasionó que el uso de herramientas tecnológicas se convirtiera en una necesidad primordial para seguir desarrollando las actividades diarias.

1.1 Delito.

El Código Penal Federal define al delito de la siguiente manera:

> Artículo 7o.- Delito es el acto u omisión que sancionan las leyes penales.

En los delitos de resultado material también será atribuible el resultado típico producido al que omita impedirlo, si éste tenía el deber jurídico de evitarlo. En estos casos se considerará que el resultado es consecuencia de una conducta omisiva, cuando se determine que el que omite impedirlo tenía el deber de actuar para ello, derivado de una ley, de un contrato o de su propio actuar precedente.

El delito es:

I. Instantáneo, cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción penal;

II.- Permanente o continuo, cuando la consumación se prolonga en el tiempo, y

III.- Continuado, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal.[1]

1.2 Delito Informático, Ciberdelito y/o Delito Cibernético.

El autor de un delito informático o ciberdelito puede ser una persona, una organización delictiva o herramientas tecnológicas diseñadas y financiadas

[1] (Cámara de Diputados del H. Congreso de la Unión)

por particulares, empresas o gobiernos con la intención de cometer un delito concreto.

"En algunos países se utiliza la expresión delitos informáticos, en otros se habla de delitos informáticos, ciberdelitos o cibercrimen o simple y llanamente delitos cometidos a través de sistemas de cómputo e Internet (computer crime)". Y para muchos también son nombrados delitos cibernéticos. [2]

Los delitos informáticos se definen como aquellos actos ilícitos en los que se usan las tecnologías de la información, como las computadoras, los programas informáticos, los medios electrónicos, el Internet, entre otros, como medio o como fin. Por ejemplo, un programa de cómputo será un medio para cometer un delito cuando es utilizado para acceder sin autorización a información confidencial; ahora bien, un programa de cómputo será el fin en un delito informático cuando recaiga sobre ese programa la conducta delictiva, como cuando se insertan virus para destruir el programa.

1.3 Ciberdelincuente.

Persona cuyo conocimiento informático le permite realizar acciones delictivas en Internet, ataca a personas, empresas, entidades particulares y gubernamentales con el propósito de realizar un fin delictivo, como lo es el robo de información, acceder a redes privadas, realizar estafas informáticas,

[2] (Martín, 2012)

suplantar identidades, producir daños informáticos, usar recursos informáticos para realizar delitos comunes contra la sociedad, entre otros.

1.4 Ciberespacio.

Es el espacio artificial creado por el conjunto de Sistemas de Información y Telecomunicaciones que utilizan las Tecnologías de la Información y las Comunicaciones; es decir de redes de ordenadores y de telecomunicaciones interconectados directa o indirectamente a nivel mundial. El ciberespacio es pues mucho más que Internet, más que los mismos sistemas y equipos, el hardware y el software e incluso que los propios usuarios, es un nuevo espacio, con sus propias leyes físicas que, a diferencia de los demás espacios, ha sido creado por el hombre para su servicio. [3]

1.5 Ciberseguridad.

La ciberseguridad pretende dar protección de aquellos elementos que dependen de las tecnologías de la información y las comunicaciones (TIC).
Es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, el que a su vez se define como el entorno complejo que resulta de la interacción de personas, software y servicios en

[3] (Feliu, 2013)

internet mediante dispositivos tecnológicos y redes conectadas a él, que no existen en cualquier forma física.

1.6 Phishing.

Termino informático por el cuan se entiende por un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos.

1.7 Malware.

Termino abreviado de "malicious software" que por su traducción se entiende como software malicioso es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.

1.8 Sexting.

Esta palabra tiene su origen en ingles que por su traducción al español se consiste en el envío de imágenes o mensajes de texto con contenido sexual a otras personas por medio de teléfonos móviles. Si bien en si mismo este acto

no es ilegal, cuando se trata de menores de edad o cuando el adulto no consiente esa actividad, constituye acto tipificado en la ley.

1.9 Stalking.

Se presenta cuando hay un acoso constante de una persona que vigila, persigue, y contacta con otra a través de medios electrónicos alterando gravemente el desarrollo de la vida cotidiana del menor y limitando su libertad de obrar.

1.10 Fraude informático.

Se refiere a un acto deliberado e ilegítimo que cause perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos, o cualquier interferencia en el funcionamiento de un sistema informático, con la intención dolosa o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona. Esta categoría de delito cibernético entraña el uso de información falsa o engañosa para obtener del objetivo algo que el autor desea o considera de valor.

1.11 Fraude bancario y con medios de pago.

Fraude bancario es un término general que abarca formas ilícitas de obtener dinero, bienes o activos que son propiedad de las instituciones financieras. El fraude con medios de pago es un tipo de fraude bancario que entraña el uso no autorizado de los datos de pago de una persona para el beneficio económico del autor. Entre los ejemplos de fraude con medios de pago se puede mencionar el fraude con tarjetas de débito y de crédito (es decir, el robo o el uso no autorizado de los datos de las tarjetas de crédito o de débito). En el caso del fraude con medios de pago, las instituciones financieras no son las únicas víctimas; también lo son los comerciantes y los clientes.

CAPÍTULO SEGUNDO

PRINCIPALES DELITOS INFORMÁTICOS POR SU MEDIO DE COMISIÓN.

En México no existe, una regulación o clasificación de conductas tipificadas expresamente como "ciberdelitos" o "delitos cibernéticos", sin embargo, la descripción típica de algunos delitos introduce elementos objetivos del tipo, que advierten el uso de instrumentos tecnológicos, en cuyo caso puedan considerarse o no como agravantes.

Como ejemplos de delitos (no limitativos) cuya comisión puede ejecutarse mediante el uso de herramientas tecnológicas pueden advertirse los siguientes:

2.1 Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Revelación de Secretos.

De acuerdo con el Código Penal Federal, el delito de revelación de secretos lo comete la persona que, sin justa causa, en perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado revele un secreto o comunicación reservada que conoce con motivo de su empleo, cargo o puesto, sanciona además a quien revele, divulgue o utilice indebidamente o en

perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada.

> Artículo 210.- Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
>
> Artículo 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial.[4]

Acceso Ilícito a Sistemas y Equipos de Informática.

Según el Código Penal Federal, el delito de acceso ilícito a sistemas y equipos de informática es cometido por quien estando autorizado o no a acceder a ellos, accede, y modifica, copia, destruye o provoca la pérdida de información contenida en esos sistemas o equipos de informática.

[4] (Cámara de Diputados del H. Congreso de la Unión)

Es importante mencionar que la legislación penal se refiere a que los sistemas o equipos de informática pueden ser propiedad de particulares, del Estado o de instituciones que integran el sistema financiero; y quienes cometen estos delitos pueden ser servidores públicos, empleados o funcionarios de las instituciones que integran el sistema financiero.

> Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copie 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 2.- Al que sin autorización modifique, destruya o provoque pérdida 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 o copie 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, protegido 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 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 un procedimiento penal resguardados por las autoridades competentes.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida 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 copie 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 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 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema 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 o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema 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 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, 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 sistema financiero, indebidamente copie información que contengan, se le impondrán 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 sistema financiero.[5]

2.2 Delitos en Materia de Derechos de Autor.

El Código Penal Federal establece que:

Artículo 4324 Bis tipifica como delito en materia de derechos de autor, la conducta consistente en fabricar con fines de lucro, un dispositivo o

[5] (Cámara de Diputados del H. Congreso de la Unión)

sistema para desactivar los dispositivos electrónicos de protección de un programa de cómputo.[6]

2.3 Engaño telefónico.

De acuerdo con el Código Penal para el estado de Veracruz, el delito de engaño telefónico consiste en el hecho de que una persona con propósito de lucro para sí o para otro, mediante una llamada telefónica o por cualquier medio electrónico, o por un mensaje electrónico pretenda engañar al receptor haciéndole creer que le va a causar o que le está causando un daño, o bien que ha privado de la libertad a un tercero.

> Artículo 173 bis. A quien con el propósito de obtener un lucro para sí o para otro, a través de una llamada telefónica o por cualquier medio electrónico, pretenda engañar a una persona haciéndole creer que le va a causar o le está causando un daño a un tercero, se le aplicarán de tres a diez años de prisión y multa de quinientos a mil días de salario. Igual penalidad se aplicará si quien realiza la llamada o envía el mensaje electrónico pretende hacer creer al receptor que le causará un daño o que se ha privado de la libertad a una persona, este delito se perseguirá de oficio. [7]

---

[6] (Cámara de Diputados del H. Congreso de la Unión)
[7] (Congreso del Estado de Veracruz)

2.4 Extorsión.

El Código Penal para la Ciudad de México dentro del articulo 236 tipifica como delito la extorsión cuando se cometiere utilizando como medio la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica, obligue a otra a dar, hacer, dejar de hacer o tolerar algo, incluso cuando se empleen imágenes, audios o videos de contenido sexual íntimo, obteniendo un lucro para sí o para otro, causando a alguien un perjuicio patrimonial.

> Artículo 236. Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de cinco a diez años de prisión y de mil a dos mil unidades de medida y actualización. Cuando el delito se cometa en contra de persona mayor de sesenta años de edad, las penas se incrementarán en un tercio. Las penas se aumentarán al doble cuando el delito se realice por servidor público miembro o ex-miembro de alguna corporación de seguridad ciudadana de cualquier nivel de gobierno. Se impondrán además al servidor o ex-servidor público, o al miembro o ex miembro de corporación de seguridad ciudadana o privada, la destitución del empleo, cargo o comisión público, y se le inhabilitará de cinco a diez años para desempeñar cargos o comisión públicos; también se le suspenderá el derecho para ejercer actividades en corporaciones de seguridad privada.

Además de las penas señaladas en el primer párrafo del presente artículo se impondrá de tres a ocho años de prisión, cuando en la comisión del delito:

I. Intervenga una o más personas armadas, o portando instrumentos peligrosos; o

II. Se emplee violencia física.

III. Se emplee cualquier mecanismo o amenaza, para hacer creer a la víctima, la supuesta intervención en el delito de algún grupo vinculado a la delincuencia organizada o asociación delictuosa sin ser ello cierto, aún y cuando ello sea solo para lograr que la víctima no denuncie el hecho.

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee imágenes, audios o videos de contenido sexual íntimo.[8]

2.5 Falsificación de Títulos o Documentos Crediticios.

El delito de falsificación de títulos o documentos crediticios consiste en el hecho de que una persona produzca, imprima, enajene, distribuya, altere o

[8] (Congreso de la Ciudad de México)

falsifique vales de papel o dispositivos electrónicos en forma de tarjeta plástica emitidos por personas morales utilizados para canjear bienes y servicios.

> Artículo 336 Se impondrán de tres a nueve años de prisión y de cien a cinco mil días multa al que, sin consentimiento de quien esté facultado para ello:
>
> VI. Adquiera, utilice o posea equipos electromagnéticos o electrónicos para sustraer la información contenida en la cinta o banda magnética de tarjetas, títulos o documentos, para el pago de bienes o servicios o para disposición de efectivo, así como a quien posea o utilice la información sustraída, de esta forma.[9]

2.6 Suplantación de identidad.

Según el Código Penal para el estado de Nuevo León, el delito de suplantación de identidad lo comete quien se atribuya por cualquier medio la identidad de otra persona u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo un daño moral, patrimonial u obteniendo un lucro indebido para sí o para otra persona.

> Artículo 444.- Comete el delito de suplantación de identidad quien se atribuya por cualquier medio la identidad de otra persona, u otorgue su

[9] (Congreso de la Ciudad de México)

consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial u obteniendo un lucro o un provecho indebido para sí o para otra persona este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil cuotas.[10]

2.7 Delito Equiparado al Robo.

Se equipará al robo el apoderamiento material o por medios electrónicos, de documentos que contengan datos de computadoras o el aprovechamiento o utilización de esos datos, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

2.8 Pornografía.

El Código Penal Federal dispone lo siguiente:

> Artículo 202 que se comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a

[10] (Congreso del Estado de Nuevo León)

realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos mil días multa. A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a

quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado. [11]

2.9 Acoso Sexual a Través de Medios Informáticos.

De acuerdo con el Código Penal para el estado de Coahuila de Zaragoza, el acoso sexual consiste en que una persona solicita para sí o para otra persona, o bien realiza una conducta sexual indeseable para quien la recibe, ya sea de manera directa o a través de medios informáticos y cause daño o el cual lesione su dignidad y coloque a la víctima en un estado de indefensión o de riesgo regulado en el siguiente artículo.

Artículo 236.- (Acoso sexual, hostigamiento sexual y privacidad sexual)

I. (Acoso sexual)

Se aplicará de dos a seis años de prisión y multa, a quien solicite favores sexuales para sí o para una tercera persona o realice una conducta de naturaleza sexual indeseable para quien la recibe, ya sea de manera directa, a través de medios informáticos, audiovisuales, virtuales o de cualquier otra forma, que le cause un daño o sufrimiento psicológico el cual lesione su dignidad, y coloque a la víctima en un estado de

[11] (Cámara de Diputados del H. Congreso de la Unión)

indefensión o de riesgo, independientemente de que se realice en uno o varios eventos.

Si la acción se realiza a través de medios informáticos, se impondrá además, la prohibición de comunicarse a través de dichos medios o redes sociales, hasta por un tiempo igual a la pena impuesta.

Las sanciones se aumentarán en un tercio más si el sujeto activo puede causar un daño personal, laboral, educativo, profesional o patrimonial; o si el sujeto pasivo del delito es una persona menor de edad o sin capacidad de comprender el significado del hecho o de decidir conforme a esa comprensión.

La misma sanción prevista en el párrafo anterior, se aplicará en el caso de que el sujeto activo fuere servidor público y utilizare los medios propios del cargo, además de la destitución e inhabilitación para ocupar empleo, cargo o comisión en el servicio público por un período de dos a seis años.[12]

2.10 Contra la Indemnidad de Privacidad de la Información Sexual.

El Código Penal Federal dispone que el delito contra la indemnidad de privacidad de la información sexual se refiere a la comunicación de contenido

[12] (Congreso del Estado de Coahuila de Zaragoza)

sexual con personas menores de dieciocho años de edad o personas que no tienen capacidad para comprender el significado del hecho o que no tienen capacidad para resistirlo.

Este delito lo comete la persona que hace uso de medios informáticos, de radiodifusión, telecomunicaciones, o de cualquier otro medio de transmisión de datos para requerir imágenes, audios o videos de actividades sexuales explícitas, actos de connotación sexual o encuentros de tipo sexual a un menor o a quien no tiene capacidad de comprender o resistir el significado del hecho.

> Artículo 199 Septies.- Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.[13]

[13] (Cámara de Diputados del H. Congreso de la Unión)

2.11 Violación a la Intimidad Sexual.

El Código Penal para el estado de Coahuila de Zaragoza tipifica el delito de violación a la intimidad sexual y establece que este delito en el articulo 236

> Artículo 236.- (Acoso sexual, hostigamiento sexual y privacidad sexual)
>
> III. (Violación a la intimidad sexual)
>
> Se impondrá de tres a seis años de prisión y multa de mil a dos mil unidades de medida y actualización, a quién con el fin de causar daño o la obtención de un beneficio sexual, por cualquier medio, divulgue, comparta, distribuya, compile, comercialice, solicite y/o publique o amenace con publicar imágenes, audios o videos de una persona desnuda parcial o totalmente, de contenido íntimo, erótico o sexual, ya sea impreso, grabado o digital, sin el consentimiento de la víctima.
>
> Se aplicarán las mismas sanciones a quienes obtengan de dispositivos móviles o dispositivos de almacenamiento físico o virtual, cualquier imagen, vídeo, textos o audios sin la autorización del titular. Estas penas se aumentarán hasta en una mitad del máximo de la pena cuando: a) El delito sea cometido por el cónyuge o por persona con la que esté, o haya estado unida a la víctima por alguna relación de afectividad, aún sin convivencia. b) Cuando el sujeto activo dada su posición de ejercicio de poder pueda causar un daño personal, laboral, educativo, profesional o patrimonial. Si se tratare de un servidor público adicionalmente será

destituido e inhabilitado para ocupar empleo, cargo o comisión públicos. c) Se cometa en contra de una persona que por su situación de discapacidad no comprenda el significado del hecho. d) Se cometa contra una persona en situación de vulnerabilidad social, por su condición cultural, étnica y/o su pertenencia a algún pueblo originario. e) Cuando se cometa con menores de edad. 138 f) A quien con violencia obligue a la víctima a fabricar, hacer el contenido íntimo, sexual o erótico publicado sin consentimiento. g) Cuando se amenace con la publicación o bloqueo de la difusión del contenido a cambio de un nuevo intercambio sexual o económico. h) Cuando un medio de comunicación impreso o digital compile o reproduzca estos contenidos y/o los haga públicos. Este delito se perseguirá por querella con excepción de lo establecido en los supuestos contemplados en los incisos a) al h). De este artículo, en estos casos el delito se perseguirá de oficio. Para los efectos de las disposiciones anteriores, la autoridad competente ordenará a la empresa de prestación de servicios digitales o informáticos, servidor de internet, red social, administrador o titular de la plataforma digital, medio de comunicación o cualquier otro donde sea publicado o compilado el contenido íntimo no autorizado, el retiro inmediato de la publicación que se realizó sin consentimiento de la víctima.

Cuando una persona con la intención de causar daño o de obtener un beneficio sexual, por cualquier medio solicite, publique, divulgue, comparta, distribuya, compile, comercialice o amenace con publicar imágenes, audios o videos de una persona desnuda total o parcialmente de contenido íntimo, erótico o sexual, ya sea impreso, grabado o digital, sin consentimiento de la víctima, comete el delito de violación a la intimidad sexual.

Además, este delito también es cometido por quienes obtengan de dispositivos móviles o dispositivos de almacenamiento físico o virtual, cualquier imagen, video, textos o audios sin autorización del titular.[14]

2.12 Difusión de Imágenes Falsificadas de Personas.

Según el Código Penal para el estado de Coahuila de Zaragoza dispone lo siguiente:

> Artículo 236 (Acoso sexual, hostigamiento sexual y privacidad sexual), el delito de difusión de imágenes falsificadas de personas se localiza como tercera fracción y contempla lo siguiente:
>
> IV. (Difusión de imágenes falsificadas de personas)
>
> Se impondrá de tres a seis años de prisión y multa de setecientos a mil doscientas unidades de medida y actualización, a quien altere, edite o

[14] (Congreso del Estado de Coahuila de Zaragoza)

modifique imágenes o videos de una persona o falsifique su perfil o datos de identidad con ánimo de mostrarla en medios informáticos en situaciones íntimas o sexuales para causarle descrédito público, vergüenza, o afectación a su honor y reputación. Estas penas se aumentarán hasta en una mitad del máximo de la pena cuando el delito se cometa contra una persona menor de edad o que carezca de la capacidad de comprender el alcance del hecho.

2.13 Delitos Contra la Libertad y la Seguridad Sexual.

Dentro del Código Penal del estado de Veracruz se localiza el delito de pederastia y la comisión de este delito cuenta con agravantes, en las cuales se localiza la de interés en el tema, haciendo mención del uso de internet, telefonía o cualquier tecnología de la información.

> Artículo 182. A quien, con consentimiento o sin él, introduzca por la vía vaginal, anal u oral el órgano sexual o cualquier otra parte del cuerpo distinta al pene o cualquier artefacto en el cuerpo de una persona menor de dieciocho años, se le impondrán de seis a treinta años de prisión y multa de hasta tres mil días de salario.
>
> A quien, sin llegar a la cópula o a la introducción vaginal, anal u oral, abuse sexualmente de un menor, agraviando su integridad física o moral, en actos públicos o privados, aprovechándose de la ignorancia,

indefensión o extrema necesidad económica o alimentaria, o de su estatus de autoridad respecto de la víctima, se le impondrán de cinco a diez años de prisión y multa de hasta doscientos cincuenta días de salario.

Artículo 183. La pederastia se considerará agravada si:

IV. El sujeto activo, para cometer este delito, mediante el uso de internet, telefonía o de cualquier otra tecnología de la información y la comunicación hubiese contactado y propuesto a la víctima un encuentro. En estos supuestos, se impondrán al activo de doce a cuarenta años de prisión y multa de hasta cinco mil días de salario. En el supuesto de la fracción III, tratándose de servidores públicos, se aplicará además la destitución e inhabilitación hasta por diez años para desempeñar empleo, cargo o comisión públicos. El responsable perderá, cuando la tenga, la patria potestad o la tutela de la víctima.[15]

[15] (Congreso del Estado de Veracruz)

CAPÍTULO TERCERO

MARCO LEGAL

Algunas de las conductas ilícitas que se identifican como Delitos Informáticos, y que se encuentran previstas y sancionadas en los Códigos Penales de las Entidades Federativas y posteriormente las que se prevén en la legislación penal federal.

3.1 Código Penal Federal.

Artículo 202.- Comete el delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, quien procure, obligue, facilite o induzca, por cualquier medio, a una o varias de estas personas a realizar actos sexuales o de exhibicionismo corporal con fines lascivos o sexuales, reales o simulados, con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o privada de telecomunicaciones, sistemas de cómputo, electrónicos o sucedáneos. Al autor de este delito se le impondrá pena de siete a doce años de prisión y de ochocientos a dos

mil días multa. A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito. La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Artículo 202 BIS.- Quien almacene, compre, arriende, el material a que se refieren los párrafos anteriores, sin fines de comercialización o distribución se le impondrán de uno a cinco años de prisión y de cien a quinientos días multa. Asimismo, estará sujeto a tratamiento psiquiátrico especializado.[16]

3.2 Ley General de Acceso de las Mujeres a Una Vida Libre de Violencia.

Tiene por objeto establecer la coordinación entre la Federación, las entidades federativas, el Distrito Federal y los municipios para prevenir, sancionar y erradicar la violencia contra las mujeres, así como los principios y modalidades

[16] (Cámara de Diputados del H. Congreso de la Unión)

para garantizar su acceso a una vida libre de violencia que favorezca su desarrollo y bienestar conforme a los principios de igualdad y de no discriminación, así como para garantizar la democracia, el desarrollo integral y sustentable que fortalezca la soberanía y el régimen democrático establecidos en la Constitución Política de los Estados Unidos Mexicanos.

3.3 Código Penal del Estado de Sinaloa.

Artículo 217. Comete delito informático, la persona que dolosamente y sin derecho:

I. Use o entre a una base de datos, sistema de computadores o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información; o

II. Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.[17]

[17] (Congreso del Estado de Sinaloa)

3.4 Código Penal del Estado de Chihuahua.

Artículo 180 Bis.

A quien reciba u obtenga de una persona, imágenes, textos o grabaciones de voz o audiovisuales de contenido erótico o sexual y las revele o difunda sin su consentimiento y en perjuicio de su intimidad, se le impondrá de seis meses a cuatro años de prisión y de cien a doscientos días de multa.

Las penas a que se refiere el presente artículo, se aumentarán en una mitad cuando el delito se cometa en contra de una persona menor de catorce años o que no tenga la capacidad de comprender el significado del hecho o que por cualquier causa no pueda resistirlo, aun y cuando mediare su consentimiento.

A quien sin haber recibido u obtenido de la víctima imágenes, textos o grabaciones de voz o audiovisuales de contenido erótico o sexual, y a sabiendas de que la información fue revelada y difundida sin el consentimiento de la víctima y aun así la difunde, se le impondrá de noventa a ciento ochenta días de trabajo a favor de la comunidad. Si la víctima es de las contempladas en el párrafo anterior, además de trabajo a favor de la comunidad, se le impondrá de seis meses a dos años de prisión.

Articulo 184 Bis.

A quien, con fines lascivos, mediante el uso de las tecnologías de la información y la comunicación o cualquier otro medio, contacte a persona menor de dieciocho años para concertar un encuentro físico u obtener imágenes, textos, grabaciones de audio o video de contenido erótico o sexual, se le impondrá de uno a tres años de prisión, de cien a trescientos días multa y el sometimiento a tratamiento integral especializado enfocado a la erradicación de la violencia sexual.

No se aplicará sanción alguna cuando la víctima sea mayor de catorce años, pero menor de dieciocho años de edad y, por su desarrollo y madurez se establezca de manera objetiva y razonable, que hubo consentimiento válido por no existir una relación asimétrica de poder o cualquier otra condición desfavorable de desigualdad respecto del sujeto activo, que viciara ese consentimiento[18]

Legislaciones en las cuales se encuentran previstos delitos informáticos

Algunos delitos informáticos se encuentran previstos en las leyes que se mencionan a continuación:

[18] (Congreso del Estado de Chihuahua)

3.5 La Ley de Instituciones de Crédito.

El que una persona sin causa legítima o sin consentimiento de quien esté facultado para ello altere, copie o reproduzca la banda magnética o medio de identificación electrónica, óptica o de cualquier otra tecnología, o sustraiga, copie o reproduzca información de tarjetas de crédito, débito, o en general cualquier otro instrumento de pago de los utilizados o emitidos por instituciones de crédito en el país o en el extranjero.

El que una persona adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida tarjetas de crédito, débito, o en general cualquier otro instrumento de pago de los utilizados o emitidos por instituciones de crédito en el país o en el extranjero, con el propósito de obtener recursos económicos, información confidencial o reservada.

El acceso de una persona sin estar facultado para ello o sin consentimiento de quien lo está, a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, alterar o modificar el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

La destrucción total o parcial que cometan los consejeros, funcionarios o empleados de las instituciones de crédito, de información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión y vigilancia de la Comisión Nacional Bancaria y de Valores.

El que los consejeros, funcionarios o empleados de instituciones de crédito, proporcionen o difundan información falsa respecto de los estados financieros de la institución de crédito, directamente o a través de cualquier medio masivo de comunicación, incluyendo medios electrónicos, ópticos o de cualquier otra tecnología.

Respecto al delito de suplantación de identidad, la Ley de Instituciones de Crédito hace referencia a que será sancionada con prisión y multa, la persona que a través de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual o de cualquier otra clase de tecnología suplante la identidad, representación o personalidad de una autoridad financiera o de alguna de sus áreas o del Sistema Bancario Mexicano, o de un servidor público, directivo, consejero, empleado, funcionario o dependiente.

También se equipará al robo el apoderamiento o uso indebido de tarjetas de crédito o débito expedidas por Instituciones Bancarias o de cualquier otra naturaleza o de títulos de crédito o documentos auténticos que sirvan para el pago de bienes o servicios o para obtener dinero efectivo sin el consentimiento de quien tenga derecho a disponer de tal instrumento.

Artículo 112 Bis.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones de crédito del país o del extranjero:

I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada.

Artículo 112 Ter.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días de salario, al que posea, adquiera, utilice, comercialice, distribuya o promueva la venta por cualquier medio, de cualquiera de los objetos a que se refiere el párrafo primero del artículo 112 Bis de esta Ley, a sabiendas de que estén alterados o falsificados.

Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o.

III. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano,

para obtener recursos económicos, información confidencial o reservada.[19]

3.6 Ley de General de Títulos y Operaciones de Crédito.

Tipifica como delitos informáticos las siguientes conductas:

El que una persona sin causa legítima o sin consentimiento de quien esté facultado para ello, altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias.

El que una persona sin causa legítima o sin consentimiento de quien esté facultado para ello, posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias, con el propósito de obtener recursos económicos, información confidencial o reservada.

---

[19] (Cámara de Diputados del H. Congreso de la Unión)

El que una persona sin causa legítima o sin consentimiento de quien esté facultado para ello, acceda, altere o modifique los equipos o medios electrónicos, ópticos o de cualquier otra tecnología de las entidades emisoras de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias, para obtener recursos económicos, información confidencial o reservada.

El que una persona sin causa legítima o sin consentimiento de quien esté facultado para ello, altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo.

Artículo 432.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, respecto de tarjetas de servicio, de crédito o en general, instrumentos utilizados en el sistema de pagos, para la adquisición de bienes y servicios, emitidos en el país o en el extranjero, por entidades comerciales no bancarias:

I. Produzca, fabrique, reproduzca, introduzca al país, imprima, enajene, aun gratuitamente, comercie o altere, cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

II. Adquiera, posea, detente, utilice o distribuya cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

III. Obtenga, comercialice o use la información sobre clientes, cuentas u operaciones de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

IV. Altere, copie o reproduzca la banda magnética o el medio de identificación electrónica, óptica o de cualquier otra tecnología, de cualquiera de los objetos a que se refiere el párrafo primero de este artículo;

V. Sustraiga, copie o reproduzca información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, o

VI. Posea, adquiera, utilice o comercialice equipos o medios electrónicos, ópticos o de cualquier otra tecnología para sustraer, copiar o reproducir información contenida en alguno de los objetos a que se refiere el párrafo primero de este artículo, con el propósito de obtener recursos económicos, información confidencial o reservada. Para los efectos de este capítulo, se entiende por tarjetas de servicio, las tarjetas emitidas por empresas comerciales no bancarias, a través de un contrato que regula el uso de las mismas, por medio de las cuales, los usuarios de las tarjetas, ya sean personas físicas o morales,

pueden utilizarlas para la adquisición de bienes o servicios en establecimientos afiliados a la empresa comercial emisora.

Artículo 434.- Se sancionará con prisión de tres a nueve años y multa de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:

I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología de las entidades emisoras de cualquiera de los objetos a que se refiere el párrafo primero del artículo 432 de esta Ley, para obtener recursos económicos, información confidencial o reservada, o

II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo que son utilizados por los usuarios del sistema de pagos, para obtener recursos económicos, información confidencial o reservada.[20]

3.7 Ley de Instituciones de Seguros y de Fianzas.

Señala que se impondrá pena de prisión y multa a los consejeros, comisarios, directores, funcionarios o empleados de una Institución o Sociedad Mutualista,

[20] (Cámara de Diputados del H. Congreso de la Unión)

que destruyan u ordenen que se destruyan, total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de inspección y vigilancia de la Comisión.

Artículo 497.- Se impondrá pena de prisión de uno a quince años y multa de 5,000 a 50,000 Días de Salario a los consejeros, comisarios, directores, funcionarios o empleados de una Institución o Sociedad Mutualista:

I. Que den en garantía los bienes del activo la Institución o Sociedad Mutualista, en contravención a lo señalado en los artículos 294, fracciones I y IV, 295, fracciones I y IV, y 361, fracciones I y IV, de esta Ley;

II. Que en sus informes, cuentas o exposiciones a las asambleas generales de accionistas o de mutualizados, falseen la situación de la sociedad;

III. Que repartan dividendos o remanentes en oposición a las prescripciones de esta Ley, independientemente de la acción para que los accionistas que las reciban, las devuelvan en un término no mayor de treinta días;

IV. Que, con el fin de falsear los reportes o información sobre la situación de la sociedad, autoricen, registren u ordenen registrar datos falsos en la contabilidad, o que proporcionen o permitan que se incluyan datos falsos en los documentos, reportes,

dictámenes, opiniones, estudios o informes que deban proporcionar a la Secretaría, a la Comisión o a las instituciones que ésta determine conforme al artículo 254 de la presente Ley, en cumplimiento a lo previsto en este ordenamiento;

V. Que destruyan u ordenen que se destruyan, total o parcialmente, los sistemas o registros contables o la documentación soporte que dé origen a los asientos contables respectivos, con anterioridad al vencimiento de los plazos legales de conservación, y

VI. Que destruyan u ordenen que se destruyan, total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de inspección y vigilancia de la Comisión.[21]

3.8 Ley del Mercado de Valores.

Sanciona a los miembros del consejo de administración, directivos, funcionarios, empleados, apoderados para celebrar operaciones con el público, comisarios o auditores externos, de un intermediario del mercado de valores, bolsa de valores, instituciones para el depósito de valores, contrapartes centrales de valores o emisoras, que destruyan u ordenen se

[21] (Cámara de Diputados del H. Congreso de la Unión)

destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de manipular u ocultar de quienes tengan interés jurídico en conocer los datos o información relevante de la sociedad, que de haberse conocido se hubiere evitado una afectación de hecho o de derecho de la propia entidad, de sus socios o de terceros.

Artículo 376.- Serán sancionados con prisión de dos a diez años, los miembros del consejo de administración, directivos, funcionarios, empleados, apoderados para celebrar operaciones con el público, comisarios o auditores externos, de un intermediario del mercado de valores, bolsa de valores, instituciones para el depósito de valores, contrapartes centrales de valores o emisoras, que cometan cualquiera de las siguientes conductas:

I. Omitan registrar en la contabilidad las operaciones efectuadas o alteren los registros contables o aumenten o disminuyan artificialmente los activos, pasivos, cuentas de orden, capital o resultados de las citadas entidades, para ocultar la verdadera naturaleza de las operaciones realizadas o su registro contable.

II. Inscriban u ordenen que se inscriban datos falsos en la contabilidad, o bien, proporcionen datos falsos en los documentos, informes, dictámenes, opiniones, estudios o

calificación crediticia, que deban presentarse a la Comisión en cumplimiento de lo previsto en esta Ley.

III. Destruyan u ordenen que se destruyan total o parcialmente, los sistemas o registros contables o la documentación soporte que dé origen a los asientos contables respectivos, con anterioridad al vencimiento de los plazos legales de conservación y con el propósito de ocultar su registro.

IV. Destruyan u ordenen que se destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión de la Comisión.

V. Destruyan u ordenen se destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de manipular u ocultar de quienes tengan interés jurídico en conocer los datos o información relevante de la sociedad, que de haberse conocido se hubiere evitado una afectación de hecho o de derecho de la propia entidad, de sus socios o de terceros. VI. Presenten a la Comisión documentos o información falsa o alterada con el objeto de ocultar su verdadero contenido o contexto, o bien, asienten o declaren ante ésta hechos falsos.[22]

[22] (Cámara de Diputados del H. Congreso de la Unión)

3.9 Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

El que una persona autorizada para tratar datos personales, con el ánimo de lucro, provoque la vulneración de seguridad de las bases de datos bajo su custodia.

El que una persona con el ánimo de lucro trate datos personales mediante engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64; VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

VIII. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

IX. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

X. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XI. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIII. Obstruir los actos de verificación de la autoridad;

XIV. Recabar datos en forma engañosa y fraudulenta;

XV. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

XVI. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

XVII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y

XVIII. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.[23]

[23] (Cámara del Diputados del H. Congreso de la Unión)

CAPÍTULO CUARTO

UNIDADES DE POLICÍA CIBERNÉTICA EN MÉXICO

Dentro de los Reglamentos Internos de Fiscalías y Secretarías de México se encuentran Unidades de Policía Cibernética o semejantes, todas ellas tienen adscripción en Direcciones y/o Unidades de Investigación e Inteligencia; en otros casos en áreas preventivas y Policías Especializadas, encargadas de dar seguimiento dentro de su jurisdicción a las actividades delictuosas informáticas que encuadren en el tipo penal, así como la prevención y seguimiento de estas conductas.

4.1 La Fiscalía General del Estado de Jalisco cuenta con una Dirección de Inteligencia.

- La Dirección General de Inteligencia Política Criminal y Prevención del Delito es la responsable de suministrar, intercambiar, y controlar la información en materia de Procuración de Justicia, para el desarrollo de sus funciones está integrado por tres direcciones, siendo la de interés la Dirección de Inteligencia la cual se localizan sus funciones y

atribuciones en los siguientes artículos del Reglamento de la Ley Orgánica de la Fiscalía del Estado de Jalisco:

Artículo 103.- La Dirección de Inteligencia tiene las siguientes atribuciones:

I. Dirigir acciones en materia de inteligencia para el desarrollo, planeación, obtención, procesamiento y aprovechamiento de la información relacionada con temas de procuración de justicia con el fin de evitar y disminuir la comisión de delitos;

II. Diseñar políticas y lineamientos para el tratamiento, suministro, intercambio, sistematización, consulta, análisis, evaluación y actualización de información que permita identificar a personas, grupos u organizaciones criminales, así como de toda aquella, que se genere sobre procuración de justicia y que pueda contribuir en la toma de decisiones;

III. Establecer las políticas y lineamientos para la instrumentación, operación y resguardo de las bases de datos de información de la Dirección, para la adopción de estrategias en materia de procuración de justicia;

IV. Definir estrategias y mantener vínculos de cooperación en materia de intercambio de información para la procuración de justicia con organismos de los tres órdenes de gobierno, nacionales e internacionales;

V. Ejecutar e instrumentar métodos de análisis de la información obtenida en materia de inteligencia operacional para prevenir y disminuir la comisión de delitos;

VI. Operar y proponer sistemas y mecanismos de análisis de la información y su recepción estratégica, que permita realizar tareas de inteligencia en materia de procuración de justicia;

VII. Identificar organizaciones criminales, su estructura y dinámica de acción que operen en el Estado de Jalisco;

VIII. Llevar a cabo acciones que permitan establecer y desarrollar los mecanismos de comunicación con instituciones de procuración de justicia de las entidades federativas o de otros países con el objeto de favorecer las tareas de cooperación en el intercambio de información;

IX. Sugerir políticas para el uso de equipos e instrumentos técnicos especializados que permitan recolectar, analizar y clasificar la información para la investigación de los delitos;

X. Llevar a cabo la vigilancia, seguimiento y procedimientos técnicos en coordinación con las unidades administrativas o con el personal operativo competente, a través de tecnología de punta que permita recopilar la información relacionada con personas, y grupos delincuenciales que contribuya en la prevención y la investigación de los delitos;

XI. Planear, previo acuerdo con la persona titular de la Fiscalía y demás superiores jerárquicos, la realización de acciones policiales y de inteligencia para la obtención, análisis y uso de información que permita identificar modos de operación delictiva y en el ámbito de su competencia, combatir la comisión de delitos;

XII. Desarrollar servicios y métodos de vigilancia e investigación proactiva para lograr la localización de personas, organizaciones o grupos que utilicen las tecnologías de información para la comisión de actos delictivos.

XIII. Adquirir, implementar y desarrollar tecnologías de información y comunicaciones que requieran los procesos de inteligencia e investigación, así como para mantener la vanguardia tecnológica en dicha unidad;

XIV. Plantear y llevar a cabo los procesos tendientes a la generación de inteligencia que permita la prevención de delitos mediante el uso de las tecnologías de información;

XV. Promover y gestionar ante las instancias correspondientes la atención de las denuncias para la prevención y combate de los delitos que se cometen utilizando medios electrónicos y tecnológicos, así como aquellos hechos ilícitos en cuya comisión se hayan utilizado dichos medios;

XVI. Realizar el análisis de sistemas y equipos informáticos y de telecomunicaciones que hayan sido utilizados indebidamente para generar, reproducir, sustraer, destruir, modificar o perder información contenida en los mismos, con la finalidad de obtener evidencia sobre el delito cometido y, en su caso, hacerlo del conocimiento de las autoridades competentes, de conformidad con las disposiciones legales aplicables en coadyuvancia con el ministerio público, y

XVII. Las demás que les corresponda, que se determinen en la Ley, este Reglamento, otras normas aplicables y las que instruya la o el Fiscal o su superior jerárquico.[24]

4.2 La Unidad de Policía Cibernética de la Fiscalía General del Estado de Coahuila de Zaragoza.

Artículo 70. De la unidad de la policía cibernética. La persona Titular de la Unidad de la Policía Cibernética, deberá contar con título de Licenciatura o Ingeniería afín; tendrá las facultades y atribuciones siguientes:

I. Coadyuvar en la investigación de hechos constitutivos de delitos cuyo objeto y/o medio

[24] (Periodico Oficial del Estado de Jalisco)

comisivo sea un sistema informático;

II. Analizar los sistemas y equipos informáticos, electrónicos y tecnológicos, vinculados

con cualquier hecho ilícito, a efecto de prevenir su comisión o investigarlo de conformidad con las disposiciones aplicables

III. Vigilar, identificar, monitorear y rastrear la red pública de Internet con el fin de prevenir y detectar conductas delictivas;

IV. Aplicar las técnicas científicas y analíticas especializadas en la recuperación de evidencias o indicios digitales para robustecer investigaciones penales;

V. Practicar las acciones necesarias requeridas por la autoridad competente para la investigación de los delitos electrónicos;

VI. Solicitar, conforme a las disposiciones aplicables, la baja de información, sitios o páginas electrónicas que representen un riesgo, amenaza o peligro para la sociedad;

VII. Requerir a las autoridades competentes en la materia, la información o documentos relativos a las bases de datos que se instruyan en la Fiscalía, que resulte útil para el ejercicio de sus funciones;

VIII. Realizar y proponer acciones para combatir los delitos cibernéticos;

IX. Promover, gestionar y dar vista al Ministerio Publico correspondiente la atención de las denuncias para la prevención y combate de los delitos que se cometen utilizando medios electrónicos y tecnológicos, así como aquellos hechos ilícitos en cuya comisión se hayan utilizado dichos instrumentos;

X. Auxiliar en la obtención y depuración de detalles de llamadas telefónicas y mensajes investigados con el debido apego a las normas correspondientes;

XI. Realizar el análisis de sistemas, equipos informáticos y de telecomunicaciones que hayan sido utilizados indebidamente o bien asegurados como material sensible con la finalidad de obtener evidencia sobre el delito cometido a efecto de coadyuvar con el Ministerio Publico para la indagatoria correspondiente, de conformidad con las disposiciones legales aplicables;

XII. Analizar los sistemas y equipos informáticos, electrónicos y tecnológicos, vinculados con cualquier hecho ilícito, a efecto de prevenir su comisión o investigarlo de conformidad con las disposiciones aplicables;

XIII. Asesorar al público en general sobre la prevención de delitos cibernéticos, y en su caso levantar actas de incidencia o reportes de atención cuando los hechos informados no constituyan delitos;

XIV. Apoyar al personal a su cargo en la realización de sus tareas; y

XV. Las demás que le encomiende el Titular de la Coordinación General de la Coordinación General de Análisis de Información y de Inteligencia Patrimonial y Económica.[25]

4.3 Dirección de Análisis de Información de la Fiscalía General del estado de Guanajuato.

Es la instancia encargada de rastrear, identificar, recabar, registrar, almacenar, procesar, clasificar, analizar, canalizar, controlar e interrelacionar información para la investigación de los delitos, conformando la base de datos y sistemas automatizados que permitan el análisis y el uso constante de la información acumulada y la implementación de estrategias o tácticas indagatorias.

Desempeña las siguientes atribuciones

Artículo 236

I. Actualizar las bases de datos y los sistemas para la recopilación y análisis de información táctica que sustenten el desarrollo de la función ministerial;
II. Vigilar el registro, manejo, actualización y control de la información que por motivos de investigación ministerial se genere;

[25] (Portal de Transparencia del Estado de Coahuila)

III. Aplicar los Protocolos de investigación y de cadena de custodia adoptados en la Fiscalía General;

IV. Clasificar la información conforme a datos, voces, documentos, constancias, reportes e imágenes vinculadas con organizaciones, grupos y personas, con motivo de hechos delictivos;

V. Relacionar la información entre las investigaciones, a través de mapas, redes de vínculos o redes técnicas;

VI. Apoyar, cuando así lo soliciten, en investigaciones que se lleven a cabo por otras instituciones de procuración de justicia y seguridad pública, previo acuerdo con la o el Director General de la AIC o la o el Fiscal General;

VII. Identificar y recabar, conforme a derecho, indicios o evidencias en equipos de cómputo o electrónicos, utilizando herramientas forenses para dar soporte a los casos e investigaciones;

VIII. Realizar informes o dictámenes de los equipos y sistemas analizados;

IX. Proveer del material necesario para apoyo a operativos e investigaciones en cuanto a vigilancia aérea y terrestre;

X. Proveer el buen uso y el mantenimiento al equipo especializado;

XI. Prestar apoyo a las actividades de las Agencias del Ministerio Público, o Unidades Especializadas de Investigación en materia de su competencia;

XII. Generar líneas de investigación tendientes a identificar y desarticular estructuras criminales;

XIII. Aportar análisis al Ministerio Público para la integración de investigaciones;

XIV. Coordinar la difusión e implementación del Modelo de Investigación Criminal;

XV. Supervisar la actualización de las bases de datos y de los sistemas para la recopilación y el análisis de información táctica que sustenten el desarrollo de la función ministerial;

XVI. Apoyar en investigaciones que se lleven a cabo por otras instituciones de seguridad pública, así como aquellas que dentro del ámbito de sus atribuciones realicen investigaciones, previa solicitud;

XVII. Recibir reportes, quejas o denuncias telefónicas o que se realicen por cualquier medio tecnológico, así como canalizarlas ante la instancia competente para su atención y seguimiento;

XVIII. Realizar la investigación de los números de identificación vehicular, así como verificar reportes o registros dentro de las bases de datos respectivas, conforme la normativa en la materia;

XIX. Recibir y canalizar reportes, quejas o denuncias de servidores y ex servidores públicos de la Fiscalía General;

XX. Recibir y canalizar los reportes del Programa Alerta AMBER Guanajuato;

XXI. Sistematizar y procesar la información con la que dispone, a fin de proporcionar informes, reportes, datos o constancias que le sean solicitados; y

XXII. Las demás que le señale el presente Reglamento Interior, los Acuerdos, Manuales de Organización, la o el Fiscal General o la o el Director General de la AIC en el ejercicio de sus atribuciones.[26]

4.4 Dirección General de la Policía Especializada y la Policía Cibernética de la Fiscalía General del estado de Chiapas.

Son atribuciones de los elementos que integran la Policía Cibernética las contempladas dentro del siguiente artículo:

Artículo 105.

I. Detectar por medio del patrullaje en la red, los sitios, procesos y responsables de las diferentes conductas delictivas que se puedan cometer en contra y a través de medios informáticos y electrónicos;

II. Orientar a la ciudadanía respecto de los pasos que deberá seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información

[26] (Periódico Oficial del Gobierno del Estado de Guanajuato)

III. Recibir y preservar todos los indicios de prueba que la víctima u ofendido aporten para el esclarecimiento de hechos y probable participación del imputado, informando de inmediato al Ministerio Público a cargo del asunto, para que éste acuerde lo conducente;

IV. Remitir al Ministerio Público como a sus superiores la información recopilada, en el cumplimiento de sus comisiones y actividades, para el debido análisis y registro;

V. Entrevistar a las personas que pudieran aportar algún dato o elemento para la investigación y esclarecimiento de los hechos que se investiguen, dentro de una carpeta de investigación asignada por el Ministerio Público;

VI. Obtener y mantener actualizado su Certificado Único Policial;

VII. Las demás que le confieran otras disposiciones o el Fiscal General.

4.5 Departamento de Información Cibernética de La Fiscalía General del estado de Chihuahua.

Dentro del Reglamento Interior de la Fiscalía General del Estado de Chihuahua se encuentra la Dirección General del Centro Estatal de Información, Análisis y Estadística Criminal, de la cual derivan tres direcciones, y para esta investigación la de interés es la Dirección de Análisis de Evidencia Digital e

Informática Forense en la cual se localiza el Departamento de Información Cibernética el cual cuenta con las siguientes atribuciones:

Art 82. Compete al Departamento de Información Cibernética:

I. Desarrollar e implementar programas en materia preventiva para el combate de los delitos electrónicos e informáticos;

II. Colaborar, con la o el Ministerio Público, a través de informes técnicos, en las investigaciones donde se identifique la comisión de un delito cibernético;

III. Vigilar, monitorear e identificar en la red pública de internet para contribuir en la prevención de conductas delictivas, en observancia de las disposiciones legales aplicables;

IV. Realizar, en el ámbito de su competencia, peritajes para determinar el mal uso y el acceso ilícito a sistemas, equipos informáticos y de comunicación;

V. Llevar a cabo, previa autorización de la autoridad jurisdiccional, la intervención de comunicaciones privadas para la investigación de delitos electrónicos e informáticos, así como aquellos hechos ilícitos en cuya comisión se hayan utilizado dichos medios;

VI. Implementar procesos basados en inteligencia para el análisis de los modos de operar de la delincuencia que utilizan medios electrónicos e informáticos;

VII. Gestionar, conforme a las disposiciones aplicables, la baja de información, sitios o páginas electrónicas que representen un riesgo, amenaza o peligro para la seguridad pública;

VIII. Promover y administrar la creación de un centro de respuesta a incidentes de seguridad informática;

IX. Examinar y catalogar la información extraída de dispositivos digitales de donde se desprendan datos sobre la comisión de un hecho ilícito en el que se hayan empleado medios electrónicos o tecnológicos;

X. Generar, con auxilio de empresas de servicios digitales, informes técnicos que aporten datos importantes para el esclarecimiento de hechos delictivos puestos a su consideración;

XI. Gestionar la adquisición de herramientas de inteligencia cibernética que permitan fortalecer las operaciones del Departamento;

XII. Promover y diseñar procedimientos relacionados a la seguridad de la información en el ámbito de su competencia;

XIII. Elaborar estudios o informes en materia de tecnologías de la información, de telecomunicaciones y de otras de naturaleza similar que

lleguen a desarrollarse y que resulten necesarias para lograr los fines de la institución, en la prevención de delitos cibernéticos;

XIV. Llevar a cabo el intercambio de información que le sea autorizada, con otras agencias de Seguridad Pública nacionales y extranjeras para el apoyo en el combate de los delitos cibernéticos;

XV. Colaborar con empresas privadas nacionales y extranjeras para la resolución de investigaciones en materia electrónica e informática conforme a las disposiciones legales; y

XVI. Las demás que le confieran las disposiciones legales aplicables, el presente Reglamento o le encomiende la persona a cargo de la Dirección.[27]

[27] (Congreso del Estado de Chihuahua)

CAPÍTULO QUINTO

CONVENIO SOBRE LA CIBERDELINCUENCIA (BUDAPEST)

Es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, o los delitos cometidos por medio de Internet, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre los países miembros del consejo de Europa y los invitados a participar en el mismo.

Está considerado como un referente obligado en los esfuerzos de la Comunidad Internacional para fortalecer y "aplicar una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional".[28]

[28] Consejo de Europa. Convenio sobre Ciberdelincuencia (Convenio de Budapest). https://www.coe.int/en/web/cybercrime/the-budapest-convention#{

5.1 Antecedentes Generales.

El 08 de noviembre de 2001, el Comité de Ministros del Consejo de Europa, adoptó el Convenio sobre Ciberdelincuencia, el cual fue presentado para su firma en la ciudad de Budapest, con fecha 23 de noviembre de 2001, entrando en vigencia el 01 de julio de 2004.

En noviembre del 2021 se realizo un segundo protocolo con el cual se actualizo el Convenio.

Actualmente, 66 Estados de Europa y los Estados Unidos de América han ratificado el Convenio, 15 Países observadores del Convenio de Budapest, encontrándose abierto a la firma de otros países invitados a participar en él.[29]

5.2 Objetivo.

Su principal objetivo es llegar a establecer una política penal común para proteger a la comunidad internacional frente a la cibercriminalidad, junto al propósito de lograr una legislación específica, también busca la creación de nuevos mecanismos de cooperación transnacional frente a los delitos cibernéticos, por lo cual establece tipos de delitos informáticos que los países miembros deben tipificar en sus legislaciones.

---

[29]Consejo de Europa. Convenio sobre Ciberdelincuencia (Convenio de Budapest). https://www.coe.int/en/web/cybercrime/the-budapest-convention#{

5.3 Contenido.

En consideración a la emergencia de amenazas cibernéticas y la especificidad de nuevos delitos, este instrumento internacional entrega una clasificación propia, organizada en cuatro capítulos que a su vez establecen tres ejes esenciales para combatir estos delitos informáticos.

Primer Eje.

Establece un catálogo con las modalidades de los delitos informáticos, es decir, define a los delitos y los clasifica de la siguiente manera:

1. La tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información, datos y los sistemas informáticos.

2. La tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales.

3. Relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

4. Relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor y a la propiedad intelectual, sin la debida autorización.

Segundo Eje.

Consiste en las normas procesales se establecen los procedimientos para salvaguardar la evidencia digital, así como también las herramientas relacionadas con la manipulación de esta evidencia, y va más allá de los delitos definidos en el punto anterior, ya que aplica a cualquier delito cometido por un medio informático o cualquier tipo de evidencia en formato electrónico, entre otras cosas determina la obtención y conservación de datos digitales para ser utilizados como pruebas.

Tercer Eje.

Normas de cooperación internacional, que son reglas de cooperación para investigar cualquier delito que involucre evidencia digital, ya sean delitos tradicionales o informáticos. Incluye, entre otras, disposiciones acerca de la localización de sospechosos, recolección o envío de evidencia digital, e incluso lo referente a extradición.

Cada Parte deberá adoptar las medidas legislativas y de otro tipo, que sean necesarias para tipificar como delito, en su derecho interno, los siguientes actos:

El acceso deliberado e ilegítimo a la totalidad o una parte de un sistema informático;

La intercepción deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas en un sistema informático;

La comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos;

La obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático;

El abuso de los dispositivos, a través de la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: un dispositivo incluido en un programa informático y una contraseña, con el fin de que sean utilizados para cometer cualquiera de los delitos indicados con anterioridad; y

La falsificación informática, el fraude informático, la pornografía infantil, los delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.

También establece que deben ser sancionadas, asimismo, las figuras de tentativa y complicidad en los delitos antes indicados, junto con explicitar la responsabilidad penal de las personas jurídicas, además, dispone que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluyendo las penas privativas de libertad.

Cada Parte mantiene la jurisdicción para juzgar los delitos objeto de la Convención, que se hubieren cometido en su territorio; a bordo de un barco o buque, una aeronave según las leyes de dicha Parte; por uno de sus nacionales, si el delito no es susceptible de sanción penal en el lugar que se cometió; o si ningún Estado tiene competencia territorial respecto del mismo. Por su parte, los aspectos referidos a la cooperación internacional en materia penal, se encuentran claramente consignados en el Convenio, contándose entre ellos el intercambio de información, la asistencia legal mutua, la colaboración en la realización de pruebas, e incluso la institución de la extradición.

5.4 Adhesiones.

El artículo 37 del Convenio señala las condiciones de Adhesión para un nuevo Miembro, facultad que tiene el Comité de Ministros del Consejo de Europa, que previa consulta con los Estados Contratantes del Convenio, y una vez obtenido su consentimiento unánime, podrá invitar a adherirse a cualquier

Estado que no sea parte del Consejo y que no haya participado en su elaboración.

Articulo 37

1. A partir de le entrada en vigor del presente Convenio, el Comité de Ministerios del Consejo de Europas podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetándola mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho de formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio, el Comité de Ministros del Consejo de Europa de conformidad con el párrafo 1 precedente, el Convenio entrara en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.[30]

[30] (Consejo de Europa)

CONCLUSIÓN.

Única. - los delitos informáticos o cibernéticos están lejos de tener una definición universal, pero siempre sin lugar a dudas existen medios por los cuales la comisión de ciertos delitos encuadra con este tipo de actividad ilegal realizada por un medio electrónico.

El aumento de las conexiones a internet en todo el mundo y la multiplicidad de dispositivos conectados hace que delitos informáticos no encuentren fronteras, ni virtuales ni físicas, situación que pone en riesgo a toda la población.

Es por ello que es indispensable establecer una estrategia para detectar y atender oportunamente los delitos cibernéticos, fortalecer las capacidades y la infraestructura tecnológica de las Instituciones para prevenir e investigar este tipo de delitos, así como desarrollar investigación científica para la prevención e investigación de los mismos, promover la creación y fortalecimiento de unidades especializadas en la prevención e investigación de delitos que se cometen por internet.

BIBLIOGRAFÍA

Congreso de la Ciudad de México. (s.f.). *Código Penal para la Ciudad de México.* Obtenido de Congreso de la Ciudad de México: https://www.congresocdmx.gob.mx/media/documentos/9cd0cdef5d5adba1c8e25b34751cccfdcca80e2c.pdf

Cámara de Diputados del H. Congreso de la Unión. (s.f.). *Codigo Penal Federal.* Obtenido de Cámara de Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Cámara de Diputados del H. Congreso de la Unión. (s.f.). *Ley de Instituciones de Crédito.* Obtenido de Cámara de Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/LIC.pdf

Cámara de Diputados del H. Congreso de la Unión. (s.f.). *Ley de Instituciones de Seguros y de Fianzas.* Obtenido de Cámara de Diputados del H. Congreso de la Unión: https://www.senado.gob.mx/comisiones/finanzas_publicas/docs/LISF.pdf

Cámara de Diputados del H. Congreso de la Unión. (s.f.). *Ley del Mercado de Valores.* Obtenido de Cámara de Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/LMV_090119.pdf

Cámara de Diputados del H. Congreso de la Unión. (s.f.). *Ley General de Títulos y Operaciones de Crédito.* Obtenido de Cámara de Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/145_220618.pdf

Cámara del Diputados del H. Congreso de la Unión. (s.f.). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* Obtenido de Cámara del Diputados del H. Congreso de la Unión: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Congreso del Estado de Chihuahua. (s.f.). *Codigo Penal del Estado de Chihuahua.* Obtenido de Congreso del Estado de Chihuahua: www.congresochihuahua2.gob.mx/biblioteca/codigos/archivosCodigos/64.pdf

Congreso del Estado de Chihuahua. (s.f.). *Reglamento Interior de la Fiscalía General del Estado.* Obtenido de Congreso del Estado de Chihuahua: http://www.congresochihuahua2.gob.mx/biblioteca/reglamentos/archivosReglamentos/260.pdf

Congreso del Estado de Chihuahua. (s.f.). *Reglamento Interior de la Fiscalía General del Estado de Chihuahua.* Obtenido de Congreso del Estado de Chihuahua: http://www.chihuahua.gob.mx/atach2/anexo/anexo_72-2018_reglamento_interior_de_la_fiscalia_general_del_estado.pdf

Congreso del Estado de Coahuila de Zaragoza. (s.f.). *Código Penal de Coahuila de Zaragoza.* Obtenido de Congreso del Estado de Coahuila de Zaragoza: https://www.congresocoahuila.gob.mx/epub/faces/Vis/Vis10.xhtml;jsessionid=UHZ20MHJMYqOJ9l9CpIS3Xz0ofo0GnoSQtydtqFj.s72-167-41-136

Congreso del Estado de Jalisco . (s.f.). *Código Penal para el Estado de Jalisco .* Obtenido de Congreso del Estado de Jalisco :

https://www.jalisco.gob.mx/sites/default/files/C%25C3%25B3digo%2520Penal%2520para%2520el%2520Estado%2520Libre%2520y%2520Soberano%2520de%2520Jalisco%2520%252826OCTU12%2529.pdf

Congreso del Estado de Nuevo León . (s.f.). *Codigo Penal del Estado de Nuevo León.* Obtenido de Congreso del Estado de Nuevo León : http://www.hcnl.gob.mx/trabajo_legislativo/leyes/pdf/CODIGO%20PENAL%20PARA%20EL%20ESTADO%20DE%20%20NUEVO%20LEON.pdf?2022-06-10

Congreso del Estado de Sinaloa. (s.f.). *Código Penal para el Estado de Sinaloa.* Obtenido de Congreso del Estado de Sinaloa: http://www.congresosinaloa.gob.mx/images/congreso/leyes/zip/codigo_penal_28-dic-2016.pdf

Congreso del Estado de Veracruz. (s.f.). *Codigo Penal del Estado de Veracruz.* Obtenido de Congreso del Estado de Veracruz: https://www.legisver.gob.mx/leyes/LeyesPDF/PENAL270115.pdf

Consejo de Europa. (s.f.). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest).* Obtenido de Consejo de Europa: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{

El Economista, Periodico digital. (s.f.). *Ciberseguridad México 2021: ransomware y robo de credenciales.* Obtenido de El Economista: https://www.eleconomista.com.mx/tecnologia/Ciberseguridad-Mexico-2021-ransomware-y-robo-de-credenciales-20220107-0046.html

Feliu, L. (2013). *Aproximacion conceptual: Ciberseguridad y Ciberdefensa. Seguridad Nacional y Cibedefensa.* Madrid: Escuela Superior de Ingenieros de Telecomunicaciones.

Interpol. (s.f.). *Ciberdelincuencia.* Obtenido de Interpol: https://www.interpol.int/es/Delitos/Ciberdelincuencia

Martín, C. V. (2012). *La Jurisdicción y Competencia Sobre Delitos Cometidos a Través de Sistemas de Cómputo e Internet.* México, D.F.: tirant lo blanch México.

Naciones Unidas. (s.f.). *Delito Cibernetico.* Obtenido de Naciones Unidas: https://www.un.org/es/events/crimecongress2015/cibercrime.shtml

Periódico Oficial del Estado de Jalisco. (s.f.). *Reglamento de la Ley Orgánica de la Fiscalía del Estado de Jalisco.* Obtenido de Periódico Oficial del Estado de Jalisco: https://periodicooficial.jalisco.gob.mx/sites/periodicooficial.jalisco.gob.mx/files/10-02-21-viii.pdf

Periodico Oficial del Estado de Jalisco. (s.f.). *Reglamento de la Ley Orgánica de la Fiscalía del Estado de Jalisco.* Obtenido de Periodico Oficial del Estado de Jalisco: https://periodicooficial.jalisco.gob.mx/sites/periodicooficial.jalisco.gob.mx/files/10-02-21-viii.pdf

Periódico Oficial del Gobierno del Estado de Guanajuato . (s.f.). *Reglamento Interior de la Fiscalía del Estado de Guanajuato.* Obtenido de Periódico Oficial del Gobierno del Estado de Guanajuato : https://normatividadestatalymunicipal.guanajuato.gob.mx/descarga_file.php?nombre

=Reglamento%20Interior%20de%20la%20Fiscal%C3%ADa%20General%20del%20Estado%20de%20Guanajuato%20(ago%202019).pdf&archivo=2e5ac40b5a02c5a2c35fe028a266aa91.pdf&id_archivo=6794

Poder Judicial del Estado de Michoacán. (s.f.). *Conceptos y antecedentes del internet y de los delitos informáticos, su clasificación y características.* Obtenido de Poder Judicial del Estado de Michoacán: https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap3.htm

Portal de Transparencia del Estado de Coahuila . (s.f.). *Ley Orgánica de la Fiscalía General del Estado de Coahuila de Zaragoza.* Obtenido de Portal de Transparencia del Estado de Coahuila : http://www.coahuilatransparente.gob.mx/reglamentos/documentos_reglamentos/REGLAMENTO%20DE%20LA%20LEY%20ORG%C3%81NICA%20DE%20LA%20FGE.pdf

Secretaria de Comunicaciones y Transportes. (s.f.). *Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo.* Obtenido de Secretaria de Comunicaciones y Transportes: https://www.gob.mx/cms/uploads/attachment/file/555226/Gui_a_de_Ciberseguridad_SCT_VF.pdf

Universidad de Cartagena - Repositorio Institucional. (s.f.). *Responsabilidad legal en materia informática: Los ciberdelitos y nuevas figuras en México.* Obtenido de Universidad de Cartagena: https://repositorio.unicartagena.edu.co/handle/11227/10253