UNIVERSIDAD VILLA RICA

ESTUDIOS INCORPORADOS A LA
UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

“REGULACIÓN DEL DELITO INFORMÁTICO EN EL ESTADO DE VERACRUZ”

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

PRESENTA:

ADRIÁN ANDRADE PAREDES

Director de Tesis
Lic. Ana Lilia González López

Revisor de Tesis
Lic. Edna del Carmen Márquez Hernández

BOCA DEL RÍO, VER. JULIO 2014

Para mi madre (†) y mi abuela, las más grandes maestras en mi vida, con amor y admiración.

ÍNDICE

Página

CAPÍTULO II

DELITO INFORMÁTICO

CAPÍTULO III

TEORÍA DEL DELITO APLICADA A LAS CONDUCTAS ILÍCITAS INFORMÁTICAS

CAPÍTULO IV
MARCO JURÍDICO NACIONAL DE LOS DELITOS INFORMÁTICOS

CAPÍTULO V
PROPUESTAS

INTRODUCCIÓN

El presente estudio es realizado como respuesta a la inquietud jurídica en materia penal que genera el rápido desarrollo de las tecnologías de la información, avances cuyos beneficios positivos son evidentes en todos los ámbitos de la vida cotidiana y que tienen como consecuencia la creación de nuevos derechos informáticos, sin embargo, también existen perjuicios negativos de estos progresos técnicos, que se reflejan en el surgimiento de novedosas formas de cometer delitos y lesionar los bienes jurídicos de la información, situación de particular interés para la comunidad jurídica veracruzana que tiene la obligación de velar por la defensa de las garantías de los ciudadanos y derivado de los conocimientos legales, proponer medidas para protegerlas.

En la primera parte de este trabajo analizaremos los diversos conceptos de delito informático que han delimitado juristas especializados en el tema para comprender los alcances de las nuevas conductas que despliegan los criminales informáticos aprovechándose de la tecnología, se conocerán múltiples clasificaciones que existen de este tipo de ilícitos que incluyen variadas maneras de perpetrarlos.

Posteriormente, la teoría del delito nos ayudará a desintegrar los componentes jurídicos de las definiciones de delitos informáticos que se encuentran vertidas en el Código Penal para el Estado Libre y Soberano de Veracruz y el Código Penal Federal, ejercicio que se realiza con el afán de percibir los elementos penales de estos preceptos y si estos defienden adecuadamente los bienes informáticos de los ciudadanos.

Seguidamente, se procederá al estudio de los códigos penales a nivel nacional que consideran a los delitos informáticos en sus textos, buscando con este recorrido jurídico reflexionar acerca de la situación de la legislación penal sustantiva actual en materia de criminalidad informática.

En la parte final de la presente exposición, se examinará el contexto actual que permea en el Estado de Veracruz respecto de los delitos informáticos, a través de estudios estadísticos respaldados y declaraciones ante la prensa de autoridades judiciales y en materia de seguridad pública, que serán referente para delimitar que existe la necesidad de modificar el código penal estatal para ofrecer una protección jurídica efectiva a los derechos informáticos de los veracruzanos, asentando una propuesta de reforma en esta materia.

CAPÍTULO I
METODOLOGÍA DE LA INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA.

En el Estado de Veracruz, existe en la actualidad una multiplicidad de conductas ilícitas que se han manifestado proporcionalmente al avance tecnológico que hoy predomina a nivel mundial, esta evolución cibernética en el entorno social si bien ha beneficiado a los ciudadanos honorables para desarrollar sus actividades cotidianas, también ha enriquecido los medios a través de los cuales las personas deshonestas delinquen, pues mediante el uso de tecnologías de información han encontrado un nicho de acción para vulnerar derechos y generar afectaciones en la esfera jurídica de los integrantes de la sociedad.

El moderno desarrollo de estos comportamientos contrarios a Derecho constituye un fenómeno de especial relevancia para la comunidad jurídica veracruzana, pues su actualización ha pasado desapercibida por la legislación penal sustantiva vigente, debido a que la tipificación de delito informático que se encuentra en el actual Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio De la Llave, no guarda identidad ni conexión con la realidad social actual pues ha sido superada por el progreso técnico y especializado de las

tecnologías de información, situación que genera una laguna legal preocupante y nociva para la tutela y protección efectiva de los bienes jurídicos de los habitantes del Estado de Veracruz, que utilizan en su vida diaria dispositivos electrónicos para intercambiar datos por medio de redes informáticas.

En este sentido, el progreso de la criminalidad informática es alarmante pues sus actores cuentan con instrumentos de vanguardia que ocasionan una afectación impune a sus víctimas, ya que sus acciones no pueden ser perseguidas ni castigadas al no estar contempladas dentro del catálogo de conductas que son reprochables como delitos dejando en completo estado de indefensión a los veracruzanos lesionados por su comportamiento contrario a Derecho al no contar con bases jurídicas sólidas que permitan combatir el crimen cibernético.

¿Está actualizada la regulación del delito informático en el Estado de Veracruz?

1.2. JUSTIFICACIÓN.

Ante el creciente avance de las tecnologías informáticas los delincuentes las utilizan para realizar conductas que afectan el patrimonio de los gobernados. Por tanto, es de gran relevancia jurídica que los comportamientos ilícitos a que afectan bienes jurídicos informáticos sean encuadrados en la legislación penal para beneficio y protección de las garantías de los ciudadanos, ya que con su tipificación se podrán perseguir y castigar generando mayor seguridad jurídica.

1.3. OBJETIVOS.

1.3.1. Objetivo general.

Estudiar las conductas que por medios informáticos pueden lesionar los derechos o intereses de los individuos y proponer una reforma al Código Penal del Estado de Veracruz en materia de delitos informáticos para que tipifique las conductas ilícitas que actualmente se generan a través del uso de las tecnologías de información.

1.3.2. Objetivos específicos.

1. Examinar el concepto jurídico de delito informático, sus características y clasificaciones.

2. Analizar los elementos de la teoría del delito aplicados a las conductas ilícitas informáticas.

3. Estudiar el marco jurídico nacional e internacional de los delitos informáticos.

4. Delimitar cómo la tipificación actual de los delitos informáticos en el Estado de Veracruz es insuficiente para castigar las conductas que actualmente se manifiestan.

1.4. HIPÓTESIS.

La tipificación de nueva conductas delictivas impulsadas por el avance tecnológico, genera la protección efectiva de los derechos de los ciudadanos que usan las tecnologías informáticas para realizar sus actividades cotidianas.

1.5. VARIABLES.

1.5.1. Variable independiente.

La tipificación de nuevas conductas delictivas impulsadas por el avance tecnológico.

1.5.2. Variable dependiente.

La generación de protección efectiva de los derechos de los ciudadanos que usan las tecnologías informáticas para realizar sus actividades cotidianas.

1.6. DEFINICIÓN DE VARIABLES.

Tipificación: descripción precisa de las acciones u omisiones que son consideradas como delito y a las que se les asigna una pena.

Nuevas conductas delictivas: comportamientos de reciente manifestación relativos a delitos.

Impulsar: promover una acción.

Avance tecnológico: aplicaciones y funciones que han adquirido los aparatos electrónicos, por medio de los inventos capaces de mejorar y evolucionar el entorno actual de las personas que los utilizan.

Generar: producir, causar, ocasionar, originar.

Protección: Defensa que se hace de alguna cosa para evitarle un daño o perjuicio.

Efectividad: capacidad para producir el efecto deseado.

Derechos: conjunto de principios, preceptos y reglas que rigen las relaciones humanas en toda sociedad civil y a los que deben someterse todos los ciudadanos,

Tecnologías de información: herramientas y métodos empleados para recabar, retener, manipular o distribuir información.

Actividad cotidiana: ocupación que ocurre con frecuencia.

1.7. TIPO DE ESTUDIO.

Estudio o modelo exploratorio o formulativo que busca facilitar una investigación precisa o el desarrollo de una hipótesis.

1.8. DISEÑO DE PRUEBA.

1.8.1. Investigación documental.

En virtud de la naturaleza propositiva, el presente trabajo de investigación se ha sustentado con material bibliográfico principalmente, por lo que se visitaron diversos centros de acopio de información.

1.8.1.1. Centros de acopio de información.

1.8.1.1.1. Biblioteca Pública Visitada.

UNIDAD DE SERVICIOS BIBLIOTECARIOS Y DE INFORMACIÓN DE LA UNIVERSIDAD VERACRUZANA.
Boulevard Adolfo Ruiz Cortines, sin número, Boca del Río, Veracruz.

1.8.1.1.2. Biblioteca Privada Visitada.

BIBLIOTECA DE LA UNIVERSIDAD VILLA RICA, Urano, sin número, Fraccionamiento Jardines de Mocambo, Boca del Río, Veracruz.

1.8.1.1.3. Biblioteca Particular Visitada.

INSTITUTO DE LA JUDICATURA FEDERAL, Avenida Juan Pablo Segundo, esquina Tiburón, Boca del Río, Veracruz.

1.8.1.2. Técnicas empleadas para la recopilación de información.

Fichas bibliográficas que contienen: nombre del autor, título de la obra, edición, editorial, país, año y páginas.

Fichas de trabajo en modalidad de transcripción que contienen: nombre del autor, título de la obra, edición, editorial, lugar, año, página (s) consultada (s) y transcripción del material de interés.

CAPÍTULO II
DELITOS INFORMÁTICOS

2.1. CONCEPTO DE DELITO INFORMÁTICO.

Para definir a los delitos informáticos, se asume que son conductas que se encuentran reguladas por la legislación penal, lo que les atribuye formalmente el carácter de delitos; aunque existen a nivel internacional países y en el plano nacional entidades federativas que carecen de dicha tipificación, sin embargo, para poder conceptualizar el comportamiento ilícito se utilizará el sustantivo delito.

Conceptualizar el crimen cibernético presenta ciertas dificultades en razón de las peculiaridades de estas conductas que engloban factores como el objetivo y la intención criminal, los medios para realizar la acción delictiva, los bienes jurídicos afectados y la naturaleza del delito, por lo que no existe una definición universal de delito informático o delito cibernético.

La trascendencia del estudio del concepto de delito informático, es consecuencia, del fenómeno de la criminalidad cibernética que actualmente permea alrededor del mundo, pues la realización de este tipo de actividades ilícitas reúne ciertos requisitos que lo delimitan, entre los que se encuentra la utilización

de un medio informático como instrumento del crimen y la finalidad de afectar al titular de un derecho informático.

La delincuencia informática es clave para establecer una concepción jurídica de los comportamientos que son dignos de reprocharse penalmente, los cuales tienen por instrumento y objeto los sistemas o técnicas de transferencia de información y datos electrónicos, los que al ser vulnerados provocan una multiplicidad de formas de lesión a una variedad de bienes jurídicos tutelados, pero no protegidos con efectividad por las normas jurídicas establecidas.

Existen diversas definiciones de las contravenciones legales en materia informática, entre ellas se encuentra la formulada por la *Organización para la Cooperación y el Desarrollo Económicos* consistente en cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos o transmisiones de datos.

Antonio Enrique Pérez Luño en su *Manual de Informática y Derecho*, conceptualizó los delitos informáticos como el agrupamiento de comportamientos delictivos que son realizados a mediante el uso de una computadora o que generan una afectación en el funcionamiento de sistemas informáticos.

De la misma forma, el jurista español Miguel Ángel Davara Rodríguez, determinó en su libro *Derecho Informático* que el delito informático es realizar una conducta en que se actualicen las características del concepto de delito, mediante un elemento informático, o vulnerando las garantías del titular de un elemento informático.

Asimismo, el investigador en Derecho Informático Julio Téllez Valdez, los define como: “actitudes contrarias a los intereses de las personas en que se tiene 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)".[1]

Para Gabriel Andrés Campoli, los delitos informáticos consisten en: "aquéllos realizados por el autor con auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o imputabilidad territorial, pero que pueden tener tipos penales específicos en algunas legislaciones, definidos con anterioridad a la aparición de los nuevos sistemas de información y telecomunicaciones".[2]

Partiendo de las anteriores definiciones se establece que el delito informático es una conducta ilícita reprochable socialmente que tiene como finalidad causar un daño a la esfera de derechos de una persona mediante la lesión de sus bienes jurídicos utilizando sistemas y técnicas informáticas, vinculadas al uso de medios electrónicos de transferencia de datos que se encuentran conectados a redes de intercambio de información.

2.2. Características de los Delitos Informáticos.

Los comportamientos delictivos que se manifiestan mediante la utilización de la tecnología y las redes de comunicación informática cuentan con diversos elementos que los distinguen de las demás conductas tipificadas, como son los siguientes:

1. Son conductas criminales de cuello blanco, en tanto que sólo determinado número de personas con ciertos conocimientos técnicos pueden cometerlas. Los sujetos que cometen el delito informático

[1] Téllez Valdés, Julio, **DERECHO INFORMÁTICO,** 4ª edición, Editorial McGraw Hill, México, 2009, p 188.
[2] Cámpoli, Gabriel Andrés, **DERECHO PENAL INFORMÁTICO EN MÉXICO,** Editorial INACIPE, México, 2004, p 17.

tienen cierto nivel socioeconómico pues deben tener acceso a una herramienta computacional así como a un servicio de conexión a *Internet* y educación tecnológica por lo que su conducta no deriva de pobreza sino de ambición.

2. Son acciones ocupacionales en cuanto a que muchas veces se realizan cuando el sujeto está trabajando. Las conductas derivan del manejo de redes de información en el trabajo, escuela y hogar de la persona que delinque puesto que en dichos espacios interactúa con los instrumentos del delito.
3. Son acciones de oportunidad porque se aprovecha de una ocasión creada o altamente intensificada en el campo de las funciones y organizaciones del sistema tecnológico y económico. Es decir, a través de tácticas de engaño y manipulación de los sistemas informáticos los delincuentes informáticos crean situaciones para encontrarse en ventaja de sus víctimas y aprovecharse de la ignorancia en el manejo de las redes.
4. Provocan serias pérdidas económicas, ya que generalmente producen beneficios millonarios a aquellos que las realizan, de acuerdo al Reporte Norton 2013 realizado por la empresa de seguridad informática Symantec en México 10 millones de personas fueron víctimas del cibercrimen con un costo de aproximadamente $4,381.00 M.N. por persona.
5. Ofrecen facilidad de tiempo y espacio, ya que pueden cometerse en milésimas de segundo y sin una necesaria presencia física. Estas situaciones comprueban la alta nocividad de dichas conductas pues se pueden manifestar a lo largo de un día un sinnúmero de veces, incluso pueden estar remotamente programadas para realizar las acciones delictivas sin que exista violencia o conocimiento del hecho.
6. Son muchos los casos y pocas las denuncias ante la falta de regulación jurídica. Debido a que no hay delito que perseguir porque

el comportamiento no se encuentra tipificado estas contravenciones legales quedan impunes dejando indefensos a los ciudadanos que son víctimas de ataques cibernéticos a sus bienes jurídicos.

7. Son muy sofisticados y relativamente frecuentes en el ámbito militar. En razón de la alta confidencialidad de la información militar y de seguridad nacional, es recurrente el quebrantamiento de los sistemas electrónicos de dichas dependencias por parte grupos delictivos altamente tecnificados.
8. Presentan grandes dificultades para su comprobación, por su carácter técnico. Lo que no es pretexto para su persecución pues la capacidad para combatir a los delincuentes informáticos debe ser proporcional a su evolución delictiva, pues la tecnología avanza para todos no solo para las personas que delinquen.
9. En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales. Ambos elementos del tipo penal se manifiestan al realizar la acción delictiva cibernéticamente, siendo predominante el que tiene la intención consciente de causar un perjuicio.
10. Ofrecen a los menores de edad facilidades para su comisión. Debido a que en la actualidad la educación básica se encuentra ligada al manejo de las computadoras, a temprana edad las personas aprendemos a manipularlas generando curiosidad en el alcance que pudieran tener en la vida diaria tanto para el bienestar de la sociedad como para su menoscabo.
11. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación a nivel internacional. Día a día se presentan nuevas formas de violaciones a derechos fundamentales a través de las redes informáticas, por tanto es de vital trascendencia implementar medidas preventivas y correctivas que garanticen la protección cibernética de los bienes de las personas que las utilizan.

Las particularidades del uso delictivo de las tecnologías de información y comunicación anteriormente descritas ponen en evidencia los aspectos jurídicos que se deben atender para reducir las amenazas cibernéticas de las que son objeto los usuarios de servicios de conexión a *Internet* pues su constante crecimiento a nivel nacional e internacional implica una demanda social para su combate.

La tendencia a la digitalización de la población es evidente e inminente, cada vez se presenta con mayor habitualidad la incorporación de la tecnología a aspectos de la vida que anteriormente funcionaban sin estos avances informáticos, un ejemplo claro es la integración de los celulares inteligentes, que cumplen una función tanto telefónica como de conexión a *Internet*, así como las pantallas de televisión que agregan a sus características la facultad de manipular sus funciones por conducto de un servicio de *Internet*; de la misma forma los vehículos automotores de modelos recientes cuentan con sistemas de conectividad inalámbrica a servidores que proporcionan diversos beneficios a sus conductores, también existen inmuebles que añaden a su diseño la última tecnología para comodidad de sus propietarios.

El introducir todos los beneficios tecnológicos a la sociedad conlleva un desarrollo moderno y tecnificado de sus integrantes, pues mejoran la manera en que se vive día con día al permitir realizar actividades financieras y servicios bancarios remotos, comunicarse rompiendo barreras transnacionales a través de una conexión a I*nternet*, libre flujo de información democrática digitalizada que promueve la libertad de expresión al no existir censura, entre otras oportunidades, que elevan la calidad de vida de los ciudadanos, sin embargo, este desarrollo viene acompañado de amenazas y ataques contra la infraestructura tecnológica, pues como ya se apuntó en la características innovadoras de los delitos informáticos, el daño que causan a la comunidad cibernética es de magnitudes enormes tanto financieras como sociales.

2.3. Sujetos del Delito informático.

La coexistencia de dos sujetos en el Derecho Penal tiene como base la conducta punible de la persona que la realiza (sujeto activo) y la que la resiente (sujeto pasivo).

En tal razón, el sujeto que es titular del bien jurídico lesionado será el sujeto pasivo y quien lesiona el derecho tutelado es el sujeto activo.

2.3.1. Sujeto activo.

El perfil de la persona que comete un cibercrimen reúne ciertas características y por lo general influyen dos situaciones, la primera el trabajo que desempeña debido a que es posible que el sujeto activo se encuentre en lugares estratégicos en los que se maneje información o procesos de carácter sensible que le permita obtener métodos para delinquir y la segunda, la habilidad para el manejo de sistemas informáticos que facilite la comisión de este tipo de delitos.

Las aptitudes del delincuente cibernético son tema de controversia, pues algunos estudiosos criminales opinan que el nivel de conocimientos técnicos no es indicador del sujeto activo de delincuencia informática, mientras que otros autores aducen que únicamente se necesitan conocimientos informáticos básicos para delinquir a través de la red.

De lo anterior se determina, que si bien los conocimientos de informática facilitan al sujeto activo la comisión de delitos en el ciberespacio, la computación actualmente es de dominio público para gran parte de los ciudadanos, lo que se corrobora con cifras del *Instituto Nacional de Estadística y Geografía* a través de la *Encuesta en Hogares sobre Disponibilidad y Uso de las Tecnologías de*

Información que reveló que 46 millones de personas utilizan *Internet* en el país al mes de abril de 2013, razón por la cual no es necesario que una persona con alto grado de estudios en informática sea considerado como el único sujeto activo, pues ante la facilidad con la que se manejan los sistemas electrónicos, cualquier individuo con mínimos conocimientos computacionales puede llegar a cometer un delito informático.

Entre los principales actores de delincuencia informática se encuentran los *hackers*, denominación que deriva del verbo en el idioma inglés *hack* que se traduce al español como “piratear”, razón por la cual también son llamados *piratas informáticos* y en la actualidad se utiliza para referirse comúnmente a los criminales informáticos debido a la utilización masiva por parte de los medios de comunicación, aunque existen diversas comunidades que por el hecho de ser apasionados de la seguridad informática no significa que tengan intenciones maliciosas.

Por lo general, los integrantes de la *comunidad hacker* son personas con conocimientos de programación, *software* y *hardware* informáticos que tienen características similares pero no únicas en su comportamiento, por tanto, es difícil emitir un concepto ante los diversos tipos de acciones que realizan, sin embargo, comparten rasgos como los siguientes:

• Tienen como principal objetivo allegarse autodidáctamente de conocimientos informáticos para uso propio.
• Dominan, modifican y exploran las tecnologías de información minuciosamente.
• Acumulan conocimientos tecnológicos y dispositivos electrónicos de última generación de una manera compulsiva y obsesiva.
• El grado de calidad de cultura informática que manejan es relativamente alto en comparación al de los usuarios comunes.

• Son perseverantes y disciplinados al fijar sus objetivos pues ante su fracaso intentan con ayuda, diversas y novedosas técnicas para culminarlos con éxito.
• Son celosos con las competencias que obtienen al practicar sus acciones pues no las ventilan a la comunidad que integran.
• Los años de vida no son un factor determinante en su capacidad.
• Son individuos que carecen de costumbres sociales especiales, como vestimenta, comportamientos aislados o estereotipo marcados.
• Su actuación no es advertida por los sistemas de seguridad informática.
• Los caracteriza la preocupación de difundir la información que obtienen que es de interés general, publicándola en páginas de *Internet*.

Existen subclases de *hackers*, que se delimitan de acuerdo al grado de conocimientos informáticos con los que cuentan y conforme a la intención de su actuar, entre ellas se encuentran:

Lamer: este tipo de usuario cibernético carece de la preparación técnica de un *hacker*, por lo que este nombre se utiliza despectivamente para nombrar a las personas con pobres conocimientos informáticos, quienes utilizan las amenazas a través de las redes como una actividad ociosa y por recreo.

Wrackers: individuos que se dedican a descargar instrumentos básicos disponibles en la red que habilitan la práctica de actividad informática nociva para perpetrar sus acciones, por tanto, la cultura cibernética que poseen es básica y al manipular estos programas generan menoscabos sin plena conciencia, lo que genera un riesgo amplio para su seguridad en la red, su actuar los convierte en un foco de ataque de virus.

Cracker: en el universo cibernético constituyen los individuos con mayor grado de peligrosidad, debido a la finalidad maliciosa de su conducta pues el acceso a bases de datos de empresas privadas y gubernamentales para obtener

ilegalmente información en su principal objetivo, la sabiduría tecnológica con la que cuentan es vasta y tienen capacidad para descifrar códigos encriptados y contraseñas con facilidad, su actuar es sin escrúpulos y con toda la intención de causar un daño y obtener un beneficio económico a cambio.

2.3.2. Sujeto pasivo.

Los sujetos que reciben un menoscabo en su esfera jurídica a través de medios electrónicos pueden ser diversos, desde una persona física, una empresa, institución crediticia y el propio gobierno son susceptibles ante las amenazas de delitos informáticos, pues la única característica que deben tener es que se encuentren conectados a una red que transfiera, comparta, genere o manipule datos e información que comprometa el bienestar de sus derechos.

Las víctimas de delincuencia cibernética son en la actualidad uno de los sectores más vulnerables a la impunidad, pues existe gran ignorancia de las necesidades de protección, así como la falta de divulgación de las posibles conductas ilícitas, lo que genera que la mayor parte de los delitos informáticos no sean castigados por la ley, sin embargo, es más frecuente su actualización por lo que es imperativo que exista una propuesta legislativa que modernice la persecución y castigo de estas conductas ilícitas contemporáneas en beneficio de los ciudadanos que utilizan cotidianamente los sistemas informáticos y que constituyen aproximadamente una tercera parte de los habitantes del país.

2.4. Bienes jurídicos protegidos en el delito informático.

La conducta del sujeto activo del delito informático pone en peligro el bien jurídico protegido de la información y como consecuencia vulnera los principales

derechos y garantías del sujeto pasivo, debido a las múltiples conductas delictivas que se pueden realizar a través de las redes.

Existe una relación innegable entre los delitos informáticos y los delitos computacionales, por tanto, es oportuno conocer su diferencia para estudiar los bienes jurídicos tutelados por los mismos.

El delito computacional es aquella conducta llevada a cabo mediante el uso de tecnologías de la información que afecta o daña bienes jurídicos ya contemplados en el ordenamiento jurídico penal, por ejemplo: el patrimonio o la seguridad sexual y únicamente se utilizan las redes cibernéticas como medio de comisión.

Mientras tanto, los delitos informáticos son aquellas conductas delictuales en las que se ataca primordialmente bienes informáticos en sí mismos, no como medio sino como fin, generando comportamientos que por su singular naturaleza no se encuadran en la descripción típica de los delitos convencionales, al resultar lesionado el bien jurídico de la información que no es solamente el acopio de la misma, sino comprende todo el proceso de almacenamiento, tratamiento y transmisión de datos.

Haciendo notar que dichos quebrantamientos si bien tienen como finalidad principal vulnerar la información como valor económico de las personas tanto físicas como morales, su afectación se traducirá secundariamente al patrimonio, como es el caso de los fraudes informáticos, violaciones a la intimidad y confidencialidad de datos, a través de la manipulación de bases de información sensible o relativa a derecho de propiedad, cuya tendencia es sustraer elementos físicos fundamentales de los sistemas informáticos y seguridad nacional, un ejemplo claro es el terrorismo informático.

La información almacenada, tratada y transmitida a través de sistemas informáticos, es el bien jurídico que realmente se protege con la regulación de los delitos informáticos, siendo necesario determinar que la información a la que se ha hecho alusión, es aquella que tiene por sí un contenido o valor económico para quien la posea.

Sin embargo, los delitos informáticos no pueden estar limitados únicamente a la protección de un bien, sino que este tipo de conducta delictiva se encuentra dentro de aquellas a las que la dogmática penal otorga el carácter de pluriofensiva atendiendo al bien jurídico de tutela penal, esto es, que produce la afectación a varios bienes jurídicos.

En ese tenor, las conductas ilícitas cibernéticas siempre irán ligadas con la información almacenada en los sistemas que se ataquen y por tal motivo tiene un carácter plural ofensivamente ya que una misma conducta puede generar un perjuicio en diversos bienes protegidos, es decir un ataque al sistema financiero, por ejemplo afectaría económicamente a las instituciones de crédito y la hacienda pública y socialmente al correcto desarrollo de las actividades monetarias de las personas, por tanto estos delitos no afectan solo a un determinado bien jurídico, sino a una multiplicidad de ellos.

2.5. Clasificaciones de los delitos informáticos.

Las particularidades jurídicas del continuo desarrollo tecnológico, la capacidad sin medida de la sociedad para utilizar herramientas informáticas y el crecimiento exponencial de su avance, se ven reflejadas en las múltiples clasificaciones de delitos informáticos que la doctrina ha concebido, las cuales son de gran ayuda para comprender adecuadamente el fenómeno de la criminalidad cibernética y hacer frente a la problemática legal que representa su combate.

Entre los diversos catálogos de conductas criminales realizadas vía informática se identifica la existencia de múltiples formas de producir un menoscabo a los bienes de un individuo informatizado y por tal motivo es importante encuadrar las acciones que vulneran derechos en las redes de información en el marco jurídico penal vigente en el Estado de Veracruz.

2.5.1. Clasificación como instrumento.

En este catálogo de delitos encuadran aquellos en los que se utiliza la computadora como medio para realizarlos, encontrando los siguientes:

1. Reproducción ilegal de documentos a través de programas computacionales.
2. Modificación de los estados financieros de empresas.
3. Emprendimiento o simulacro de delitos convencionales.
4. Hurto de derechos de uso de un ordenador.
5. Conocimiento, filtración o plagio de información privada.
6. Alteración de datos de entrada y de salida.
7. Usufructo ilegítimo o quebrantamiento de una codificación cibernética para ingresar a un sistema con fórmulas informáticas inadecuadas.
8. Desviación de divisas hacia cuentas bancarias apócrifas.
9. Uso sin derecho de software.
10. Introducción de órdenes informáticas que generan paralizaciones en la lógica interna de sistemas computacionales, con la finalidad de conseguir un provecho.
11. Variación en la operación de programas informáticos.
12. Adquisición de datos mediantes residuos impresos en papel o en cinta magnética posteriormente a la realización de actividades computacionales.
13. Penetración a sitios computarizados sin autorización.

14. Intromisión de líneas de transferencia de información.

2.5.2. Clasificación como fin.

Los comportamientos que dirigen a afectar a las computadoras como un bien mueble material son catalogados de acuerdo a sus objetivos finales, como lo son:

1. Bloquear totalmente un sistema.
2. Destruir programas instalados por medio de cualquier método.
3. Dañar la memoria del ordenador.
4. Daño físico al hardware.
5. Sabotaje o terrorismo en el que se destruya o apodere de los centros neurálgicos computarizados.
6. Secuestro de soportes de información valiosa con fines de chantaje.

2.5.3. Ataques a los sistemas de información.

Como sistema de información se consideran las computadoras personales autónomas, agendas electrónicas personales, teléfonos celulares, intranets, extranets, redes, servidores y otras infraestructuras de *Internet*.

La *Comisión de las Comunidades Europeas*, en su comunicado *Seguridad de las redes y de la información: propuesta para un enfoque político europeo*, detalló las amenazas contra los sistemas informáticos de la siguiente manera:

1. Acceso no autorizado a sistemas de información.- consiste en la entrada sin permiso del propietario a una red desarrollándose de diversas formas como

ataques directos o bien adueñándose de contraseñas, archivos confidenciales para posteriormente usarlos y aprovecharlos ilegítimamente, es la llamada piratería informática.

2. Perturbación de los sistemas informáticos.- son métodos que entorpecen el uso de los sistemas y no permiten usarlos correctamente deteriorando los servicios ofrecidos en *Internet*, entre ellos se encuentran los ataques de negación de servicio que tiene por objeto sobrecargar los servidores con mensajes generados automáticamente.
3. Ejecución de programas informáticos perjudiciales que modifican o destruyen datos.- Los más conocidos son los virus, bombas lógicas, troyanos y gusanos, los cuales son aplicaciones cibernéticas que se infiltran en las computadoras y traen como consecuencia la alteración o destrucción de la información que se encuentra archivada en su memoria.
4. Intercepción de las comunicaciones.- es la intromisión malintencionada en el envío y recepción de mensajes electrónicos, captación de información almacenada en bases de datos que causa un grave perjuicio a la intimidad de los usuarios de los sistemas de información.
5. Declaraciones falsas.- entre estos ataques se encuentra la usurpación de identidad con la finalidad de causar un daño y la posibilidad de proporcionar datos ficticios en la red que propicien fraudes electrónicos mediante compras en la red o ilícitas transferencias de fondos.

2.5.4. Tipos de delitos informáticos reconocidos por las Naciones Unidas.

El *Octavo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente* que tuvo como marco la ciudad de La Habana, Cuba y abarcó del veintisiete de agosto al siete de septiembre de mil novecientos noventa, fue la reunión de académicos jurídicos internacionales en la que la

Asamblea General de Naciones Unidas adoptó una resolución que tenía por objeto la legislación contra el ciberdelito.

Basándose en la Resolución 45/121 (1990) las Naciones Unidas publicaron en mil novecientos noventa y cuatro un *Manual sobre la prevención y el control de delitos informáticos*, en la que se advierte que clasificaron las conductas ilícitas de la forma que a continuación se ilustra:

Delitos	Características
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de datos de entrada	Fraude informático más comúnmente conocido también como sustracción de datos, es fácil de cometer y difícil de descubrir, no requiere conocimiento técnico de informática y lo realiza la persona que tiene acceso al procesamiento de datos en la fase de adquisición de los mismos.
Manipulación de programas	Difícil de descubrir ya que el delincuente debe tener conocimientos técnicos de informática, consiste en modificar programas informáticos existentes para que puedan realizar una función no autorizada al mismo tiempo que su función
Manipulación de datos de salida	Para efectuar este delito se fija un objetivo al funcionamiento del sistema informático, conlleva la falsificación de instrucciones para los ordenadores y

	codificación de información electrónica falsificada.
Falsificaciones informáticas	
Como objeto	Cuando se alteran datos de documentos almacenados en forma computarizada.
Como instrumento	Cuando las computadoras se utilizan para efectuar falsificaciones de documentos de uso comercial, los cuales son de tal calidad que solo un experto puede diferenciarlos de los auténticos.
Daños o modificaciones a programas computarizados	
Sabotaje informático	Acto de borrar, suprimir o modificar sin autorización, funciones o datos de computadoras con la intención de obstaculizar el funcionamiento normal del sistema. Las técnicas para cometerlo son: virus, gusanos y bomba lógica o cronológica.
Virus	Serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros.
Gusanos	Análogo al virus en la característica de infiltración en programas informáticos legítimos para destruir o modificar datos, es diferente del virus porque no puede regenerarse.

Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en un futuro, son difíciles de detectar antes de que exploten y por eso poseen el máximo potencial de daño.
Falsificaciones informáticas	
Acceso no autorizado a sistemas o servicios	Motivados por la simple curiosidad como en el caso de muchos piratas informáticos hasta el sabotaje o espionaje informático.
Piratas informáticos o hackers	Acceso desde un lugar exterior situado en la red de telecomunicaciones, aprovechando la falta de rigor de las medidas de seguridad para tener acceso, el descubrimiento de deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.
Reproducción no autorizada de programas informáticos de protección legal	Problema que ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas.

2.5.5. Clasificación del Convenio sobre la Ciberdelincuencia en Europa.

El principal instrumento jurídico europeo de cooperación en materia de delincuencia informática es conocido informalmente como el *Convenio de Budapest*, el cual fue emitido el veintitrés de noviembre de dos mil uno, dentro de los cuarenta y ocho artículos que lo constituyen observando cuatro variantes de infracciones:

1. Delitos contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos.
2. Delitos informáticos.
3. Delitos relacionados con el contenido.
4. Delitos relacionados con infracciones de la propiedad y de los derechos afines.

Los criterios para la segmentación anterior de los delitos informáticos son diversos, por lo que la coherencia de la clasificación no es total, puesto que las tres categorías iniciales tienen como factor el objeto que se protege jurídicamente, mientras que la restante resalta el método que se utiliza para perpetrar el delito.

Dentro de los *Delitos contra la confidencialidad, la integridad y disponibilidad de los datos y sistemas informáticos*, se dilucidan una variedad de conductas ilícitas, entre ellas:

- Acceso ilícito mediante piratería de sistemas y programas.
- Espionaje de datos.
- Intervención ilícita.
- Manipulación de datos.
- Ataques contra la integridad del sistema.

Por otra parte, los delitos relacionados con el contenido comprenden elementos ilícitos propios de la información que se maneja a través de las redes, entre ellos están:

- Material erótico o pornográfico con exclusión de la pornografía infantil.
- Pornografía infantil.
- Racismo, lenguaje ofensivo y exaltación de la violencia.
- Delitos contra la religión.
- Juegos ilegales y juegos en línea.
- Difamación e información falsa.
- Correo basura y amenazas conexas.
- Otras formas de contenido ilícito.

Asimismo, los derechos de autor y de propiedad industrial del material que se difunde *vía Internet* al estar a disposición de un enorme público tienen el riesgo de ser objeto de falsificaciones y piratería. Los comportamientos que se manifiestan en este rubro contemplan:

- Delitos en materia de derechos de autor.
- Delitos en materia de marcas.

Los delitos informáticos son una categoría en la que se han englobado la mayoría de las acciones contrarias a Derecho que se realizan cibernéticamente, sin embargo, en estricto sentido, son aquellos en los que se utiliza un sistema informático para perpetrarlos, se delimitan de la siguiente manera:

- Fraude informático.
- Falsificación informática.
- Robo de identidad.
- Utilización indebida de dispositivos.

CAPÍTULO III
TEORÍA DEL DELITO APLICADA A LAS CONDUCTAS ILICÍTAS INFORMÁTICAS

3.1. CONCEPTOS GENERALES DE TEORÍA DEL DELITO.

La teoría del delito estudia los componentes jurídicos que se presentan habitualmente en los hechos delictivos, con la finalidad de establecer si se configura una conducta ilícita o esta no llega a constituirse.

El doctor Eduardo López Betancourt define a la teoría del delito "como una parte de la ciencia del Derecho Penal que comprende el estudio de los elementos positivos y negativos del delito, así como sus formas de manifestarse. Los elementos positivos del delito configuran la existencia de éste, mientras que los elementos negativos constituirán su inexistencia; las formas de manifestación, se refieren a la aparición del mismo." [3]

Al delito se le atribuyen múltiples componentes que lo construyen en su totalidad, la doctrina a través de estudios de más de un siglo en varias etapas los ha sintetizado en siete elementos cada uno de ellos con su correspondiente

[3] López Betancourt, Eduardo, **TEORÍA DEL DELITO,** 15ª ed, Editorial Porrúa, México, 2008, p 3.

aspecto positivo y negativo, es decir, cuando se trata de los elementos positivos se está ante la indudable existencia del delito y al abordar los elementos negativos, se encuentra la inexistencia del ilícito.

Entre los elementos positivos que determinan la presencia del delito aparecen los siguientes:

- La conducta.
- La tipicidad.
- La antijuricidad.
- La imputabilidad.
- La culpabilidad.
- La punibilidad.

De la misma forma, los elementos negativos que se consideran en la teoría del delito para establecer su inexistencia son:

- La ausencia de conducta.
- La atipicidad.
- Las causas de justificación.
- La inimputabilidad.
- La inculpabilidad.
- Las excusas absolutorias.

Al examinar las principales partes que componen el delito, no se niega que estos factores al unirse constituyen el hecho delictivo en una totalidad, sin embargo al analizar cada aspecto por separado, se logra comprender la conexión que existe entre ellos e identificar si las conductas contrarias a Derecho que se presentan en las relaciones humanas constituyen un ilícito al actualizarse los

elementos positivos o se excluyen de las figuras delictivas al comprender elementos negativos.

3.2. ESTUDIO DE LOS ELEMENTOS ESENCIALES DEL DELITO EN LOS TIPOS PENALES DE DELITO INFORMÁTICO.

Para fines prácticos del presente estudio, se examinarán las tipificaciones de delito informático contenidas en el *Código Penal para el Estado de Veracruz* y *Código Penal Federal* a la luz de la teoría del delito y sus elementos, tanto positivos como negativos.

El delito informático en el *Código Penal para el Estado de Veracruz*, se encuentra comprendido de la siguiente manera:

"Artículo 181.-Comete delito informático quien, sin derecho y con perjuicio de tercero:- I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o- II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.- Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad."

Por otra parte, el *Código Penal Federal* contempla a los delitos informáticos de acuerdo a los preceptos siguientes:

"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.- 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.- Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.- Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.”

En los subcapítulos siguientes, se analizan los preceptos legales transcritos atendiendo a la literalidad de la descripción del comportamiento humano que afecta el bien jurídico de la información, la cual fue realizada por el

juzgador federal y veracruzano en los códigos penales correspondientes, con la finalidad de comprender el crimen informático, mediante una reflexión de su composición a la luz de los elementos positivos y negativos del delito.

Al estudiar las bases teóricas penales del artículo 181 del *Código Penal para el Estado de Veracruz*, se observa una protección básica al ciudadano de la intimidad de su información.

De la misma forma, al examinar los conceptos punitivos que integran los artículos 211 bis 1 al 211 bis 7 del *Código Penal Federal*, se estima que la defensa a los derechos de confidencialidad de información de los gobernados guarda similitud con la legislación estatal, sin embargo, protege en mayor magnitud al Estado y las entidades financieras, generando una desproporción con la tutela realizada a las personas físicas integrantes de la sociedad que utilizan medios de informáticos en sus actividades cotidianas.

3.2.1. Conducta y ausencia de conducta.

El elemento positivo que da origen al delito es la conducta por ser el comportamiento humano requerido para la existencia del ilícito.

La ausencia de conducta es su enfoque contrario, que deriva en la inexistencia del delito debido a vicios en el actuar del sujeto activo.

3.2.1.1. Conducta

La conducta es el primer elemento básico del delito, y se define como “el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.”[4]

La anterior definición establece que únicamente los seres humanos pueden realizar conductas tanto positivas como negativas, por medio de una actividad o una inactividad, siendo voluntarias porque carecen de una imposición al sujeto otorgándole libertad para decidir efectuarlas, siempre con una finalidad implícita en el propósito de su acción u omisión.

Otra manera de conceptualizar la conducta es “el comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.”[5]

“La acción consiste en un acto de voluntad, su exteriorización mediante un hacer o mediante inactividad, y el resultado será la modificación producida en el mundo exterior o el peligro creado con dicha conducta. De lo que se desprende el nexo causal entre la acción y el resultado.” [6]

Tomando en consideración las definiciones anteriores, se concluye que al actualizarse la conducta se manifiestan tres elementos, que son:

1. Un comportamiento de hacer o no hacer.
2. Una consecuencia.
3. Un vínculo de motivación entre el comportamiento y la consecuencia.

---

[4] Op. Cit., p 83.
[5] Castellanos Tena, Fernando, **LINEAMIENTOS ELEMENTALES DE DERECHO PENAL,** 46ª ed, Editorial Porrúa, México, 2005, p 149.
[6] Op. Cit. Nota 3, p 85.

Existen dos formas a través de las cuales se puede manifestar la conducta en los delitos: la acción y la omisión.

3.2.1.1.1. Delito de acción.

El delito de acción es la actividad realizada por un ser humano que produce resultados en el mundo jurídico a través de un movimiento voluntario.

Al ser el hombre el único individuo que goza de voluntad es el sujeto activo que monopoliza el delito, castigándose por el Derecho solo sus acciones corporales externas, pues los pensamientos e intenciones carecen de sanción penal.

Al actuar del sujeto se le atribuyen dos características que lo distinguen: la primera es la física que conlleva un movimiento, la segunda es psíquica y lo constituye la conciencia de actuar, generando con esta actividad voluntaria un resultado el cual tiene un nexo con la conducta.

3.2.1.1.2. Delito de omisión.

La omisión consiste en la falta de actividad del sujeto de manera voluntaria, cuando la ley ordena realizar un acto determinado.

"La voluntad en la omisión consiste en querer no realizar la acción esperada y exigida, es decir, en querer la inactividad, o realizarla culposamente. En consecuencia, en la omisión, existe al igual que en la acción, en su caso, un elemento psicológico: querer la inactividad o llevarla a cabo en forma culposa."[7]

---

[7] Porte Petit Candaudap, Celestino, **APUNTAMIENTOS DE LA PARTE GENERAL DEL DERECHO PENAL,** 19ª ed, Editorial Porrúa, México, 2001, p 240.

Al no realizar la conducta, sin coacción alguna, el sujeto genera una consecuencia con su no hacer, cuando este tiene una obligación legal de actuar.

En la omisión existen dos hipótesis que se manifiestan:

- Omisión simple.- consiste en ignorar una ley, es decir incumplir con un mandato legal sin que exista un resultado material, sino jurídico violando una norma reglamentaria, por ejemplo el encubrimiento.

- Omisión por comisión.- se le atribuye a la inactividad del sujeto que causa un menoscabo en la esfera jurídica de otra persona al abstenerse de realizar una conducta exigida por la ley, por ejemplo, la omisión de socorro que trae como consecuencia el deceso de una persona.

3.2.1.2. Conducta en el delito informático.

Una vez establecido que la conducta como elemento positivo del delito constituye la acción u omisión del sujeto activo, que tiene como resultado la afectación de derechos de terceras personas, existiendo un nexo entre el comportamiento y la consecuencia jurídica de menoscabo; del análisis de los artículos 181 del *Código Penal del Estado de Veracruz* y 211 bis del *Código Penal Federal*, se advierte que se está ante la presencia de una conducta de acción, pues para realizarlos es necesario un movimiento corporal.

En la legislación penal sustantiva veracruzana, el numeral citado delimita la conducta de acción al incorporar verbos que obligadamente requieren de impulso físico para consumarse; en la fracción I se hallan: ingresar, obtener, conocer, utilizar, alterar, reproducir; de la misma forma en la fracción II se

asentaron actividades positivas como interceptar, interferir, usar, alterar, dañar y destruir.

Por otra parte, la ley punitiva del orden federal en el artículo mencionado determina un ejercicio de conducta efectivo que modifique, destruya, conozca, copie o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, hechos que únicamente se ejecutan a través de una acción.

3.2.1.3. Ausencia de conducta.

La ausencia de conducta es elemento negativo que consiste en la falta de acción o bien en una omisión al realizar un ilícito.

Este aspecto negativo del delito se puede presentar por tres causas, las cuales son:

1. Fuerza física superior exterior irresistible.- es un supuesto jurídico en el cual el ser humano participa en un hecho, pero sin la intervención de su voluntad, porque está sometido a una fuerza tal que le impide por completo moverse voluntariamente.

2. Fuerza mayor.- se configura cuando el sujeto realiza una conducta delictiva de acción u omisión coaccionado por una fuerza física proveniente de la naturaleza.

3. Movimientos reflejos.- son actos corporales involuntarios que generan un hecho delictivo.

Aunado a las anteriores causas negativas, diversos autores consideran al sueño, el hipnotismo y el sonambulismo, como fuente de ausencia de conducta.

El sueño es un estado fisiológico de autorregulación y reposo uniforme de un organismo, por tanto, al estar dormido el sujeto carece de voluntad y dominio sobre sí mismo.

El hipnotismo es un procedimiento para producir el llamado sueño magnético, por fascinación, influjo personal o por aparatos personales, en consecuencia, al igual que en el sueño se manifiesta una falta de conciencia del sujeto de delinquir.

Por último, el sonambulismo es un trastorno de la conducta durante el sueño asociado con el desarrollo de actividades motoras automáticas que pueden ser sencillas o complejas, sin que se produzca una interrupción del sueño, sin que al despertar se recuerde algo, de tal manera que en ese estado psíquico no se actúa conscientemente.

3.2.1.4. Ausencia de conducta en el delito informático.

El aspecto negativo de la conducta, consistente en su ausencia es sumamente difícil que sea atribuible a los delitos informáticos, debido a la característica fundamental de acción que tienen los mismos.

El que exista una fuerza física superior exterior irresistible o fuerza mayor que vicie la voluntad de la persona que comete el delito informático es inaceptable, pues se requieren diversos procedimientos técnicos que se deben seguir para consumar un ilícito de esta índole, lo mismo ocurre con los movimientos reflejos, es decir, un fenómeno de la naturaleza no va a traer como consecuencia

inminente que una persona cometa un fraude informático, o una persona al esquivar un objeto por inercia ingresará sin autorización a un sistema de información.

La actualización de un delito informático, requiere una capacidad de su actor para manipular instrumentos que permitan su realización, por tanto, es innegable que se debe estar plenamente consciente para llevar a cabo la conducta, por lo que sería sumamente complejo que un individuo dormido, sonámbulo o bajo hipnosis, pueda consumar un ilícito informático.

3.2.2. Tipicidad y atipicidad.

La tipicidad es la adecuación de la conducta a la descripción legal del delito plasmada en la ley.

Su aspecto negativo es la atipicidad, consistente en la falta de encuadre del comportamiento real a la hipótesis jurídica contenida en la legislación por omisión de alguno de los elementos característicos que lo componen.

3.2.2.1. Tipicidad.

La vida diaria nos presenta una serie de hechos contrarios a la norma y que, por dañar en alto grado la convivencia social, se sancionan con una pena. “El código o las leyes los definen y los concretan para poder castigarlos. Esa descripción legal, desprovista de carácter valorativo según el creador de la teoría, es lo que constituye la tipicidad.”[8]

[8] Jiménez de Asúa, Luis, **LECCIONES DE DERECHO PENAL,** Obra Compilada y Editada, Editorial Pedagógica Iberoamericana, México, 1995, p 154.

“La tipicidad es la adecuación de una conducta concreta con la descripción legal formulada en abstracto.” [9]

De las anteriores definiciones se obtiene que la tipicidad consiste en que la conducta realizada por una persona sea la misma que se describe como delito en la ley penal.

Este elemento positivo es vital para el delito, pues si no existe una adecuación del comportamiento desplegado al asentado en la legislación, es inminente la inexistencia del crimen.

La tipicidad tiene su fundamento constitucional en el párrafo tercero del artículo 14 de la Carta Magna que enuncia lo siguiente: “En los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata”.

“La diferencia entre tipicidad y tipo penal radica en que la primera se refiere a la conducta y el segundo pertenece a la ley, a la descripción o hipótesis plasmada por el legislador sobre un hecho ilícito; es la fórmula legal a que se debe adecuar la conducta para la existencia de un delito.”[10]

[9] Op. Cit. Nota 5, p 167.
[10] Op. Cit. Nota 3, p 118.

3.2.2.2. Tipicidad en el delito informático.

La tipificación del delito informático reside en la adecuación de una conducta de acción realizada por un sujeto activo, que se manifiesta con la totalidad de los elementos del tipo penal descrito por el legislador en el artículo 181 del *Código Penal para el Estado Libre y Soberano de Veracruz* o en su caso en los numerales 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7 del *Código Penal Federal*.

3.2.2.3. Clasificación de los delitos de acuerdo al tipo penal.

Los delitos se pueden clasificar de acuerdo al tipo penal de la siguiente forma:

- Por su composición:
  - Normales.- conformado de elementos objetivos.
  - Anormales.- constituido de elementos objetivos y subjetivos.
- Por su ordenación metodológica:
  - Fundamentales.- formados con una conducta ilícita sobre un bien jurídico tutelado.
  - Especiales.- contienen el tipo fundamental, agregándole un elemento distintivo sin subordinación.
  - Complementados.- requieren la realización previa de un tipo fundamental.
- Por su Independencia:
  - Autónomos.- tipos con plena independencia que no necesitan la actualización de algún otro.
  - Subordinados.- requieren la existencia de otro tipo.
- Por su formulación:

- Casuísticos.- se plantean diversas formas de realizar el delito, se subdividen en:
  - Alternativos: se proyectan dos o más hipótesis y con ejecutar una de ellas se configura la conducta ilícita.
  - Acumulativos: se exige realizar todas las hipótesis previstas para encuadrar la conducta al tipo.
- Amplios.- disponen una figura única para adecuar todas las formas de ejecución del delito.

- Por el daño que causan:
  - De lesión.- generan una afectación apremiante al bien jurídicamente protegido.
  - De peligro.- no es necesario un perjuicio, es suficiente poner en riesgo un derecho tutelado.

3.2.2.4. Clasificación del tipo penal del delito informático.

Conforme a la clasificación del delito de acuerdo al tipo descrito anteriormente, los delitos informáticos se categorizan de esta forma:

1. Composición anormal debido a que incorporan elementos tanto objetivos como subjetivos y normativos.

a. Objetivos.- se encuentran los verbos que describen al delito tales como alterar, dañar y destruir, también el objeto jurídico afectado que será la información y el material en que recaerá la acción como bases de datos, sistemas de informática o red de computadoras.
b. Normativos.- los enunciados sin autorización y sin derecho, contienen una valoración jurídica del comportamiento que presume su ilicitud.

c. Subjetivos.- al estipular el legislador que la conducta será en perjuicio de un tercero y que la información se encuentra protegida por un medio de seguridad, asume que el actuar del sujeto activo es doloso con todo el ánimo de causar un daño.

2. Ordenación metodológica especial ya que es conformado por un tipo penal básico y una característica que genere un tipo penal con una nueva denominación pero sin subordinación; dentro de la legislación estatal veracruzana los delitos informáticos están contemplados en el título IV que corresponde a los delitos contra la intimidad personal y la inviolabilidad del secreto, mientras que en el ordenamiento penal federal se ubican en el titulo noveno que se denomina revelación de secretos y acceso ilícito a sistemas y equipos de informática, lo que corrobora que los delitos informáticos son especiales al estar su estructura complementada por un tipo básico y peculiaridades tecnológicas que lo definen.
3. Autonomía subordinada, al depender su configuración de otros tipos fundamentales como el daño en propiedad ajena, fraude, robo, entre otros.
4. Formulación casuística alternativa, debido a que del análisis del artículo 211 bis 1 del *Código Penal Federal* y del numeral 181 del *Código Penal para el Estado Libre y Soberano de Veracruz*, es evidente que para actualizarse el delito informático se pueden realizar diversas conductas dañinas de derechos, sin que sea necesaria la configuración total de estas, pues con realizar una de ellas estamos ante la presencia de un acto delictivo.
5. Resultado de daños de lesión, puesto que el comportamiento desplegado con cometer un delito informático tendrá como resultado la violación de la información ocasionando un deterioro en ese bien jurídico tutelado.

3.2.2.5. Elementos del tipo penal.

Grandes estudiosos del Derecho Penal en México, específicamente el doctor Eduardo López Betancourt, señala como elementos del tipo penal los siguientes:

- “El presupuesto de la conducta o el hecho.
- El sujeto activo.
- El sujeto pasivo.
- El objeto jurídico.
- El objeto material.
- Las modalidades de la conducta.
    - Referencias temporales.
    - Referencias espaciales.
    - Referencia a otro hecho punible.
    - De referencia de otra índole.
    - Medios empleados.
- Elementos normativos.
- Elemento subjetivo del injusto”.[11]

3.2.2.5.1. Presupuesto de la conducta o hecho.

La conducta antijurídica que el legislador describe en los tipos penales informáticos es detallada por los hechos objetivos del comportamiento, es decir, con su representación desde el punto de vista externo.

[11] Op. Cit. Nota 3, p 127.

El elemento objetivo del tipo penal que se traduce en el presupuesto de la conducta o el hecho, se identifica plenamente con la manifestación de la voluntad en el mundo físico que es requerida por el tipo penal para configurar un delito.

"Los elementos objetivos podemos entenderlos como aquellos que proceden del mundo externo perceptible por los sentidos, es decir que tiene la característica de ser tangibles, externos, materiales, por lo que también podríamos decir que son objetivos los que representan cosas, hechos o situaciones del mundo circulante."[12]

3.2.2.5.2. Sujeto activo y sujeto pasivo.

El sujeto activo es el individuo quien realiza la conducta delictiva, en este caso el delincuente informático que perpetre el ilícito, mientras tanto el sujeto pasivo consistirá en aquella persona que es ofendida ante quien recae la conducta antijurídica realizada por el maleante de la información.

3.2.2.5.3. Objeto jurídico y objeto material.

El objeto jurídico es considerado el bien protegido por la ley penal, consiste en aquellos derechos que el legislador valora e intenta proteger al determinar una figura delictiva, entre estos bienes tutelados se encuentran: el patrimonio, la libertad y la vida.

El objeto material, es la persona o cosa en la que se percibe materialmente la acción, también se le conoce como el objeto de la conducta.

---

[12] Plascencia Villanueva, Raúl, **TEORÍA DEL DELITO,** 3ª reimpresión, Instituto de Investigaciones Jurídicas, México, 2004, p 106.

"El objeto material del delito es la persona o cosa sobre la que recae el delito. Lo son cualquiera de los sujetos pasivos o bien las cosas animadas o inanimadas, mientras tanto, el bien jurídico es el objeto de la acción incriminable."[13]

3.2.2.5.4. Modalidades de la conducta.

Las referencias temporales se manifiestan en los tipos penales cuando se incluye en la descripción de la conducta delictiva una situación de tiempo, por consiguiente se necesita un determinado estado transitorio ya sea en la sociedad o en el individuo que afecte directamente el desarrollo de su conducta.

Un ejemplo de referencia temporal se encuentra incluido en el delito de ultrajes a la autoridad contemplado por el artículo 331 del *Código Penal para el Estado Libre y Soberano de Veracruz*, el cual especifica que se impondrán de seis meses a dos años de prisión y multa hasta de cuarenta días de salario a quien amenace o agreda a un servidor público en el momento de ejercer sus funciones o con motivo de ellas. La referencia temporal radica en que la conducta ilícita se realiza al estar en activo el servicio público desplegado por el sujeto pasivo.

Las referencias espaciales aparecen cuando la legislación especifica el sitio o lugar para la comisión del delito, un ejemplo claro es el delito de abigeato previsto por el artículo 210 de la legislación sustantiva penal veracruzana, que determina que a quien en el medio rural se apodere de una o más cabezas de ganado, sin consentimiento de quien legalmente pueda disponer de ellas, se le impondrán de seis a doce años de prisión y multa hasta de trescientos días de

[13] Carrancá y Trujillo Raúl, Carrancá y Rivas Raúl, **DERECHO PENAL MEXICANO (PARTE GENERAL),** 23ª ed, Editorial Porrúa, México 2007, p 295.

salario mínimo. En este caso la referencia espacial consiste en la población agropecuaria en la que se llevará a cabo el delito.

Los medios de ejecución del tipo penal son atribuidos a mecanismos de acción determinados en los delitos para que pueda encuadrar la conducta en la descripción contenida en la ley, es decir, cuando el comportamiento contrario a Derecho se ejecuta a través de la forma en que expresamente se tipifica, son las maneras de comisión del delito que el legislador apunta en la definición del delito.

3.2.2.5.5. Elementos normativos.

El elemento normativo se funda en el enfoque legal con el que se tienen que mirar las palabras incluidas en el tipo penal, apreciación que contiene una valoración jurídica del comportamiento que presume que es contrario a Derecho.

"Los elementos normativos son una llamada de atención al juez, en los que se le trata de advertir que debe confirmar la antijuricidad de la conducta, ya que con estos elementos, un hecho aparentemente lícito puede pasar a ser un hecho ilícito; asimismo, puede ocurrir lo contrario, es decir, que un hecho aparentemente ilícito no lo sea."[14]

Los autores mexicanos Fernando Castellanos Tena y Celestino Porte Petit dividen los elementos normativos, en atención al contenido de su valor en:

1. Valoración normativa.- Atendiendo al sentido de los vocablos que emanan del ámbito jurídico.
2. Valoración cultural.- Considerando el significado de las palabras de acuerdo al área de estudio de las que provienen.

[14] Op. Cit. Nota 3, p 133.

3.2.2.5.6. Elementos subjetivos.

Los elementos subjetivos del tipo penal van a atender a la intención, al ánimo que tuvo el sujeto activo o que debe tener, en la realización de algún ilícito penal, es decir, atienden a las circunstancias que se dan en el mundo interno, a la psiqué del autor. El fundamento de este elemento, se halla en la conciencia y en la voluntad del actor del delito, pues este tiene conocimiento pleno de la ejecución y las consecuencias de su acto delictuoso.

3.2.2.6. Elementos del tipo penal del delito informático.

Los componentes de las tipificaciones de delito informático contenidas en el artículo 211 bis 1 del *Código Penal Federal* y del numeral 181 del *Código Penal para el Estado Libre y Soberano de Veracruz*, son vitales para el estudio de este apartado pues estos elementos serán el marco donde encuadre la conducta ilícita con precisión jurídica para que pueda ser considerada como delito.

3.2.2.6.1. Presupuesto de la conducta o del hecho del delito informático.

Del diseño conductual del delito informático que se observa en la ley punitiva del estado veracruzano y la legislación penal de la federación, en que se delimita la ilicitud del comportamiento a través de distintos verbos que originan una percepción real de la acción antijurídica, entre estos se ubican los siguientes: obtener, conocer, utilizar, alterar, interceptar, interferir, usar, dañar, destruir, modificar y provocar pérdida, vocablos que permiten llevar al plano físico la intención de delinquir del sujeto activo.

3.2.2.6.2. Sujeto activo y sujeto pasivo del delito informático.

En la tipografía penal del estado de Veracruz y la del orden federal, se encuentra que cualquier persona puede ser sujeto activo del delito informático, siempre y cuando tenga la capacidad para adentrarse en una base de datos, soporte lógico, programa informático, sistemas o equipos de informática.

Por otro lado, el sujeto activo en dichas legislaciones penales será aquella persona que cuente con alguno de los medios tecnológicos de recopilación de información descritos, sin embargo, el *Código Penal Federal* establece personas morales específicas en las que puede recaer la acción ilícita informática, en los artículos 211 bis 2, 211 bis 3, protege al Estado mexicano de este comportamiento, de igual manera el 211 bis 4 y 211 bis 5, le atribuye la calidad de sujeto pasivo a las entidades que conforman el sistema financiero de nuestro país.

3.2.2.6.3. Objeto jurídico y objeto material del delito informático.

El bien jurídico tutelado por los delitos informáticos consiste en la intimidad y salvaguarda de la información recopilada en sistemas de intercambio de información.

De la misma forma, el objeto material en el que recae la conducta de los ilícitos informáticos son los datos incluidos en la información, el propio sistema de intercambio de información como red para su transferencia y también como aparato tecnológico.

3.2.2.6.4. Modalidades de la conducta del delito informático.

Dentro de los tipos penales informáticos que constituyen la base de este estudio no se encuentra alguna referencia temporal o espacial que exija su configuración.

De acuerdo a lo contenido en los tipos de los delitos informáticos correspondientes al *Código Penal Veracruzano* y al del orden federal, existen diversos medios mediante los cuales se pueden ejecutar, se manifiestan al ingresar a una base de datos, sistema o red de computadoras con el fin de obtener, conocer, utilizar, alterar o reproducir información y la modificación, destrucción o pérdida de información contenida en sistemas o equipos de informática.

3.2.2.6.5. Elementos normativos del delito informático.

En los artículos 211 bis 1 del *Código Penal Federal* y 181 del *Código Penal para el Estado Libre y Soberano de Veracruz*, se aprecian los elementos normativos los determinan.

Como elementos de valoración normativa aparecen, los enunciados: sin derecho y sin autorización, los cuales otorgan una connotación de ilegalidad a la conducta.

Asimismo, los elementos de valoración cultural son variados debido a las particularidades de estos ilícitos que conllevan un aspecto novedoso y actual para el plano del Derecho Penal, ligado directamente con el avance tecnológico de la sociedad, entre ellos se presentan: base de datos, sistema o red de computadoras, soporte lógico o programa informático, sistemas o equipos de

informática, palabras que no corresponden al lenguaje jurídico, por lo que para conocer su significado es necesario tener ciertos conocimientos técnicos de las tecnologías de información.

Aunado a estos elementos, se manifiestan en los tipos penales informáticos términos ambiguos, los cuales es importante que se aclaren para delimitar con exactitud las conductas penales que se lleguen a encuadrar en ellos, la principal palabra a la que se le puede otorgar un matiz diverso es *información*.

Información es un vocablo al cual se le pueden dar amplios sentidos, etimológicamente se conforma de dos partes: *in* y *formatio*. En latín *formatio* se refiere a la acción de formar o de dar forma, de generar algo, por su parte, el prefijo *in* indica dirección hacia dentro.

De acuerdo a la *Real Academia de la Lengua Española*, se define como: "1.f. Acción y efecto de informar. 5. f. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada".

Desde el punto de vista de la ciencia de la computación, la información es "un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del ente que posee dicha información con su entorno."[15]

Asimismo, de acuerdo al artículo 3, fracción V de la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, información se

[15] http://es.wikipedia.org/wiki/Información, 24 de febrero de 2014.

entiende como: “la contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título”.

La palabra información implica un bien jurídico que es tendiente a adjudicarse, el cual contiene un valor intrínseco y la integran diversos archivos como imágenes, texto, audio, video, claves confidenciales, que pueden ser personales, privados, empresariales o gubernamentales, por tal motivo, es un término que debe estar claro por el juzgador para valorarlo al momento en que esté frente a un delito informático, pues la delimitación de su alcance es vital para decidir si existe una conducta delictiva.

3.2.2.6.6. Elementos subjetivos del delito informático.

En las tipificaciones penales del estado de Veracruz y de la Federación se evidencian características que generan la convicción de que el sujeto activo del delito informático actúa dolosamente; estos elementos consisten en que la conducta se realice con perjuicio de tercero y con fines de lucro, así como que el bien jurídico tutelado se encuentre en equipos de informática protegidos por algún mecanismo de seguridad, puesto que es necesario el ánimo de causar un menoscabo para violentar estos sistemas.

3.2.2.2. Atipicidad.

La falta de encuadramiento de una conducta en el tipo penal deriva en su atipicidad, mientras que la falta de tipo consiste en la inexistencia de la descripción del comportamiento en la ley.

Jiménez de Asúa, manifiesta: “Ha de afirmarse, pues, que existe ausencia de tipicidad en estos dos supuestos: a) Cuando no concurren en un hecho concreto todos los elementos del tipo descrito en el Código Penal o en las leyes penales, y puesto que son varias las relaciones y elementos de los tipos, distintas son también las hipótesis que pueden concebirse (atipicidad propiamente dicha)- b) Cuando la ley penal no ha descrito la conducta que en realidad se nos presenta con característica antijurídica (ausencia de tipicidad, en sentido estricto)”.[16]

Conforme a lo considerado por el doctor Eduardo López Betancourt, para encontrar las atipicidades, se deben señalar los elementos negativos del tipo penal, siendo los siguientes: “I. Ausencia del presupuesto de la conducta o del hecho.- II. Ausencia de la calidad del sujeto activo exigido en el tipo.- III. Ausencia de la calidad del sujeto pasivo exigido en el tipo.- IV. Ausencia del objeto jurídico.- V. Ausencia del objeto material.- VI. Ausencia de las modalidades de la conducta.- a. De referencias temporales.- b. De referencias espaciales.- c. De referencia a otro hecho punible.-d. De referencia a otra índole exigida por el tipo.- e. De los medios empleados.- VII. Ausencia del elemento normativo.- VIII. Ausencia del elemento subjetivo del injusto.” [17]

Como efectos de la atipicidad, existen tres supuestos:

- Falta de integración del tipo penal.- generando la no existencia del hecho delictivo.
- Traslación del tipo penal.- no se actualiza un elemento de la descripción dando lugar a una variante del delito.
- Configuración de un ilícito imposible.- cuando se carece del bien jurídico protegido.

[16] Op. Cit. Nota 3. pp 140 y 141.
[17] Ibidem. p 142.

3.2.2.3. Atipicidad en el delito informático.

En los delitos informáticos tipificados en la legislación estatal veracruzana y en la federal se observan los elementos objetivos, normativos y subjetivos de los tipos penales, por consiguiente existirá atipicidad cuando el comportamiento realizado por un individuo no encuadre perfectamente con las características jurídicas delictivas que describe el legislador en los artículos que los contemplan.

Es incorrecto señalar que existe una ausencia del tipo penal informático en dichas leyes punitivas, puesto que están incluidas conductas ilícitas que se castigan y por ende protegen al bien jurídico de la información, sin embargo, ya que el avance tecnológico es cada vez más acelerado y las formas de vulnerar este derecho están en constante modernización, el tipo penal descrito ha quedado rezagado y no se ajusta a la realidad contemporánea que se vive, pues los riesgos de ser sujeto pasivo de los delitos informáticos, aumentan día con día, dejando desprotegidos a los ciudadanos que utilizan las tecnologías de información cotidianamente, al existir una ventana de impunidad para los delincuentes informáticos puesto que su conducta maliciosa es muchas veces atípica al carecer de los elementos anticuadamente considerados, por tal motivo para proporcionar una protección efectiva a la intimidad y salvaguarda de la información recopilada en sistemas de intercambio de información, es necesario actualizar el tipo penal acorde con la vanguardia del momento tecnológico en que se encuentra la sociedad contemporánea.

3.2.3. Antijuricidad y causas de justificación.

"La antijuricidad es lo contrario a Derecho. El ámbito penal, precisamente radica en contrariar lo establecido en la norma jurídica."[18]

"El aspecto negativo de la antijuricidad lo constituyen las causas de justificación, que son las razones o circunstancias que el legislador consideró para anular la antijuricidad de la conducta típica realizada, al estimarla lícita, jurídica o justificativa."[19]

3.2.3.1. Antijuricidad.

La antijuricidad es la contravención del ordenamiento jurídico penal, es el elemento positivo que constituye la esencia de la conducta ilícita, cuando un comportamiento se contrapone a la ley es antijurídico y como consecuencia se considera delito por la sociedad.

Analizando las raíces etimológicas de la palabra antijuricidad obtenemos que deriva del latín *anti*, que tiene como significado, lo contrario y de *juridice*, que quiere decir Derecho, por tanto, ir en contra del Derecho es su definición etimológica.

La antijuricidad es lo contrario a Derecho, por lo tanto, no basta que la conducta encuadre en el tipo penal, se necesita que esta conducta sea antijurídica, considerando como tal a toda aquella definida por la ley, no protegida por causas de justificación, establecidas de manera expresa en la misma.

---

[18] Amuchategui Requena, Griselda Irma, **DERECHO PENAL,** 3ª ed, Editorial Oxford, México, 2005, p 73.
[19] Op. Cit., p 74.

Este elemento positivo del delito ha sido dividido por la doctrina en dos corrientes:

1) Positivismo jurídico.- concibe la antijuricidad como un concepto legal y la denomina como formal.

2) Positivismo sociológico.- considera a lo contrario a Derecho como un concepto de la sociedad y la titula como material.

"La antijuricidad formal o nominal, es el acto formalmente contrario al Derecho, en tanto que es trasgresión de una norma establecida por el Estado, de un mandato o de una prohibición del orden jurídico."[20]. Lo que se traduce en una contravención directa a la legislación penal.

"La antijuricidad material, será materialmente contrario al Derecho cuando esté en contradicción con los fines del orden jurídico que regula la vida común; esta lesión o riesgo será materialmente legitima, a pesar de ir dirigida contra los intereses jurídicamente protegidos, en el caso y en la medida en que responda a esos fines del orden jurídico, y, por consiguiente, a la misma convivencia humana. Ese contenido material (antisocial) de la infracción es independiente de su exacta apreciación del legislador."[21]. Consiste en el menoscabo sociológico directo que afecta el interés colectivo.

3.2.3.2. Antijuricidad en el delito informático.

En el uso de las tecnologías de información, las redes electrónicas y el *Internet*, se descubren una multiplicidad de conductas que son materialmente

[20] Jiménez de Asúa, Luis, **LA LEY Y EL DELITO,** 11ª ed, Editorial Sudamericana, Argentina, 1980, p 207.
[21] Op. Cit., p 278.

dañinas para la sociedad, por este motivo los legisladores del estado de Veracruz y los integrantes del Congreso de la Unión, incluyeron en los códigos penales correspondientes, descripciones de estos comportamientos contrarios a Derecho que tienden a proteger la confidencialidad de los datos que se transmiten a través de esos medios, dándole el carácter formal de antijuricidad necesario para su combate.

De tal modo que la antijuricidad se manifiesta en los delitos informáticos cuando la conducta típica desplegada por el sujeto activo del delito, contraviene lo dispuesto por los artículos 181 del *Código Penal del estado de Veracruz* y 211 bis I al 211 bis 7 del *Código Penal Federal*.

3.2.3.3. Causas de justificación.

"Cuando en un hecho presumiblemente delictuoso falta la antijuricidad, podemos decir: no hay delito por la existencia de una causa de justificación, es decir, el individuo ha actuado en determinada forma sin el ánimo de transgredir las normas penales."[22]

El elemento negativo de la antijuricidad son los motivos que hacen lícita la acción del sujeto activo, pues su comportamiento se torna ajustado a Derecho, por tanto no lesiona bien jurídico alguno.

"Las causas de justificación son aquellas condiciones que tienen el poder de excluir la antijuricidad de una conducta típica. Representan un aspecto negativo del delito; en presencia de alguna de ellas falta uno de los elementos esenciales del delito, a saber: la antijuricidad."[23]

---

[22] Op. Cit. Nota 3, p 153.
[23] Op. Cit. Nota 5. p 183.

En el *Código Penal Federal*, se encuentran estipulados los motivos de licitud en el artículo 15, fracciones III, IV, V y VI, que disponen: "…III.- Se actúe con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:- a) Que el bien jurídico sea disponible;- b) Que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo; y- c) Que el consentimiento sea expreso o tácito y sin que medie algún vicio; o bien, que el hecho se realice en circunstancias tales que permitan fundadamente presumir que, de haberse consultado al titular, éste hubiese otorgado el mismo;- IV.- Se repela una agresión real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se defiende.- Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente, al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien, lo encuentre en alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión;- V.- Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo;- VI.- La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro;…"

De los numerales anteriores se concluye que las causas de justificación que radican en el Derecho positivo mexicano consisten en:

- Consentimiento del titular del bien jurídico afectado.- cuando el propietario de un derecho otorga la facultad a otra persona de disponer libremente del mismo.
- Legítima defensa.- es el combate al ataque amenazador de un derecho, por parte del individuo que se ve agredido en contra de su agresor, respetando las dimensionas de las acciones precisas para su protección.
- Estado de necesidad.- es la salvaguarda de un bien jurídico tutelado que se manifiesta agrediendo otro bien igualmente protegido por la ley.
- Cumplimiento de un deber o ejercicio de un derecho.- consiste en la realización de una conducta que pudiera ser contraria a Derecho de no estar regulada como lícita por un ordenamiento jurídico.

3.2.3.4. Causas de justificación del delito informático.

En los crímenes relativos a la información que se han estudiado en el presente capitulo pueden operar distintas causas de ilicitud.

Por lo que respecta al consentimiento del titular del bien jurídico afectado, si bien pudiera darse el caso de que se justifique la conducta por esta razón, en ambos delitos tanto del orden estatal como el federal, se observa el elemento del tipo normativo; sin derecho y sin autorización, por consiguiente, más que una causa de licitud estaríamos ante la presencia de una atipicidad de la conducta por no encuadrar en el tipo penal al carecer del mencionado elemento normativo.

Es factible argumentar que la persona que cometa un ilícito informático realizó sus acciones en legítima defensa para repeler una agresión a su confidencialidad de datos, pues si este sujeto pasivo tiene la capacidad y los conocimientos técnicos para combatir la amenaza a sus derechos, es lógico que active los mecanismos a su alcance para impedir un agravio a su información,

aunque su conducta implique violar los sistemas de seguridad informáticos del individuo que lo está atacando.

En relación al estado de necesidad, existe la posibilidad de su actualización al justificarse el ingreso a una base de datos sin autorización y realizar alguna acción prevista por los tipos penales de delitos informáticos violentando el bien jurídico de la información, con la finalidad de proteger un diverso bien amparado por la ley, siempre que no exista algún otro medio que ocasione menos perjuicios.

Tocante al cumplimiento de un deber o ejercicio de un derecho, es posible que esta causa de ilicitud se configure siempre y cuando quede demostrado fidedignamente la obligación necesaria y acreditada del sujeto activo para violentar la intimidad y salvaguarda de la información recopilada en sistemas de intercambio de datos.

3.2.4. Imputabilidad e inimputabilidad.

Es imputable el individuo que goza de salud mental y se encuentra libre de circunstancias que alteren su comprensión, teniendo la edad señalada por la legislación para ser responsable de un crimen.

La postura negativa es la inimputabilidad traducida como la carencia de voluntad y comprensión en el ámbito penal.

3.2.4.1. Imputabilidad.

"La imputabilidad es la capacidad de querer y entender, en el campo del Derecho Penal. Querer es estar en condiciones de aceptar o realizar algo voluntariamente, y entender es la capacidad mental y la edad biológica para desplegar esa decisión." [24]

La definición de imputabilidad contenida en el Diccionario Jurídico del Departamento de Derecho del Instituto Tecnológico de Monterrey Campus Estado de México es la siguiente: "Capaz penalmente, Individuo a quien cabe atribuirle un delito por la conciencia, libertad, voluntad y lucidez con la que ha obrado".[25]

Para que a un individuo se le impute un delito debe tener la capacidad de desear las consecuencias de su actuar, así como de entender las afectaciones que provocará con su conducta; para que estos componentes de la acción sean válidos es indispensable que el sujeto se encuentre en pleno goce de sus facultades mentales y que cuente con la mayoría de edad para ejercer sus derechos.

Existen dos componentes imprescindibles para la imputabilidad, el primero es el elemento intelectual o de conocimiento, que radica en la capacidad de comprensión de lo injusto, es decir el carácter ilícito del hecho, el segundo consiste en el elemento de la voluntad, que es conducirse de acuerdo con esa comprensión, por lo que la conjunción de estos dos elementos sustentan la imputabilidad.

---

[24] Op. Cit. Nota 3, p 180.
[25] http://www.cem.itesm.mx/derecho/referencia/diccionario/bodies/i.htm, 4 de marzo de 2014.

3.2.4.2. Imputabilidad en el delito informático.

En ese sentido, tanto en el Código Penal para el Estado Libre y Soberano de Veracruz como en el Código Penal Federal, se determina que los mayores de dieciocho años de edad y los que al momento de realizar la conducta típica tengan capacidad para comprender el hecho ilícito son personas que se les puede imputar crímenes informáticos.

3.2.4.3. Inimputabilidad.

La incapacidad de un individuo para querer cometer un ilícito y la falta de noción de su acción constituye la óptica negativa de la imputabilidad.

Luis Jiménez de Asúa sostiene que: “Son causas de inimputabilidad la falta de desarrollo y la salud de la mente, así como los trastornos pasajeros de las facultades mentales que privan o perturban en el sujeto la facultad de conocer el deber; esto es, aquellas causas en las que si bien el hecho es típico y antijurídico, no se encuentra el agente en condiciones de que se le pueda atribuir el acto que perpetró.”[26]

Entre los motivos de inimputabilidad, se encuentra la clasificación de Luis Jiménez de Asua, que los divide de la siguiente forma:

- Inmadurez mental:

  - Menores.- los individuos con minoría de edad están sujetos a un régimen penal diverso que se funda en una acción tutelar por parte del Estado, atendiendo a su falta de capacidad de ejercicio.

[26] Ibídem, p 191.

- Trastorno mental.- es la carencia de desarrollo de la plena conciencia, así como del pensamiento y voluntad, que impide una adecuada proporción entre la edad física y la edad intelectual de una persona.

- Trastorno mental transitorio: es una perturbación de las facultades mentales pasajera, de corta duración.

- Falta de salud mental: se caracteriza por la enfermedad de la psique que padece el sujeto activo del delito.

La inimputabilidad la hallamos en la fracción VII del *Código Penal Federal* que establece:

"…VII. Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquél o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible."

3.2.4.4. Inimputabilidad en el delito informático.

La inimputabilidad de los delitos informáticos se manifestara como causal de exclusión del ilícito, si la conducta antijurídica tipificada es desplegada por una persona que cuente con menos de dieciocho años de edad o un individuo que carezca de facultades para entender las consecuencias de su comportamiento, debido a una afección psicológica o física, por encontrarse viciado el actuar de estos sujetos y por ende no podrá ser castigado por el Derecho Penal, en su caso, su conducta será corregida por las leyes de menores infractores o de acuerdo a la

legislación que compete a los seres humanos que cuentan con una deficiencia mental.

3.2.5. Culpabilidad e inculpabilidad.

"La culpabilidad es la relación directa que existe entre la voluntad y el conocimiento del hecho con la conducta realizada."[27]

La inculpabilidad se define como la ausencia de reproche jurídico penal de una conducta.

3.2.5.1. Culpabilidad.

"En amplio sentido puede definirse la culpabilidad como el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica." [28]

La culpabilidad se determina por el vínculo psíquico o mental que existe entre la intención de la conducta realizada por el delincuente y la recriminación legal de dicho comportamiento.

"La culpabilidad se traduce en el nexo intelectual y emocional que liga al sujeto con su acto."[29]

De acuerdo a Ignacio Villalobos, en su libro *Derecho Penal Mexicano* la culpabilidad, por lo general es el insulto del sujeto al orden jurídico y por los

[27] Op. Cit. Nota 18, p 91.
[28] Op. Cit. Nota 8, p 234.
[29] Op. Cit. Nota 5, p 234.

preceptos y restricciones que lo constituyen y conservan, insulto que aparece voluntariamente en el dolo, o involuntariamente en la culpa.

Existen tres enfoques doctrinales para estudiar la naturaleza de la culpabilidad, estos son:

1. Teoría psicológica.- Corriente penal que fundamenta la culpa en aspectos únicamente de índole intelectual, se limita a valorar la actitud del sujeto activo frente al resultado material del delito.

2. Teoría normativa.- Doctrina que reprueba la intención de una conducta para generar culpabilidad, al vínculo psíquico entre el agente del delito y su comportamiento, se adiciona la reprochabilidad de su actuar por un ordenamiento jurídico.

3. Teoría finalista.- Ideal que afirma que la culpabilidad es únicamente la censura de la conducta, dejando de considerar los deseos del delincuente como elementos de esta, trasladándolos al tipo.

3.2.5.1.1. Especies de culpabilidad.

La culpabilidad aparece jurídicamente de dos maneras, a través del dolo y la culpa.

“Constituyen auténticas especies en las que encarna conceptualmente el género abstracto de la culpabilidad.”[30]

[30] Op. Cit. Nota 8, p 238.

En el dolo, el criminal sabiendo con plena conciencia las consecuencias de sus acciones sin coerción alguna decide ejecutarlas.

En la culpa consciente, el sujeto realiza su conducta esperando que las consecuencias de la misma no se generen, mientras que en la culpa inconsciente, el agente carece de la previsión del resultado de su comportamiento, existiendo una falta de cuidado por el respeto de derechos de terceros.

3.2.5.1.2. Dolo.

"El dolo existe cuando se produce un resultado típicamente antijurídico, con conciencia de que se quebrante el deber, con conocimiento de las circunstancias de hecho y del curso esencial de la relación de causalidad existente entre la manifestación humana y el cambio en el mundo exterior, con voluntad de realizar la acción y con representación del resultado que se requiere o ratifica."[31]

En la anterior definición se observan los elementos del dolo que lo componen: el intelectual y el emocional.

El elemento intelectual del dolo radica en el conocimiento del sujeto activo del delito de que sus acciones son contrarias a derecho y el elemento intelectual se funda en la voluntad mental de crear un resultado antijurídico.

Dentro de la concepción doctrinal del dolo se encuentra la siguiente clasificación planteada:

[31]Op. Cit. Nota 8, p 243.

- En cuanto a la modalidad de la dirección:
  - Dolo directo.- Cuando se requiere la conducta o el resultado. Es decir, el dolo se caracteriza en querer el resultado, si es delito material, y en querer la conducta, si es delito formal.
  - Dolo eventual.- Hay una representación del resultado, pero no hay voluntariedad del mismo, porque no se quiere el resultado, sino se acepta en caso de que se produzca.
  - Dolo de consecuencia necesaria.- Cuando queriendo el resultado, se prevé como seguro otro resultado derivado de la misma conducta.
- En cuanto a su extensión:
  - Determinado.- Cuando la intención se dirige directamente al delito que se comete.
  - Indeterminado.- Cuando la intención no es enfocada a un delito exclusivo, derivando en múltiples afectaciones jurídicas.
- En cuanto a su nacimiento:
  - Inicial o precedente.- Es aquel que ya existe antes de la consumación del delito.
  - Subsiguiente.- Se presenta cuando el sujeto empieza una acción de buena fe, y después acontece un deseo antijurídico que lo lleva a incurrir en un delito.
- Por su intensidad:
  - Genérico.- Al encauzar la voluntad a producir un resultado jurídicamente prohibido.
  - Especifico.- Cuando la acción tiene un fin especial que distingue la lesión cometida de otro antijurídico.
- Dependiendo de su duración:
  - Dolo del ímpetu.- Cuando la acción sigue inmediatamente a la intención.
  - Dolo simple.- Cuando el sujeto activo del delito, lleva la idea de realizar la conducta ilícita, prepara todos los medios necesarios para la realización del hecho antijurídico y para la obtención del resultado esperado.

- Dolo de propósito.- Consiste en la intención premeditada y perseverante de realizar el delito, acompañado de la ordenación previa de los medios de comisión.

- En cuanto a su contenido:
- De daño.- Cuando el resultado que el agente produce, es la destrucción o disminución real de un bien jurídico.
- De peligro.- Se genera cuando el sujeto, encamina su actuar a un daño y su producto culmina únicamente en un riesgo.
- De peligro con resultado de daño.- La voluntad es orientada a ocasionar un peligro, sin embargo, la conducta es castigada cuando se comprueba un daño.

Del anterior catálogo, se aprecia la diversidad de fórmulas en las que una intención dolosa puede adecuarse, atendiendo a sus principales características, lo que permite una adecuada delimitación de la intención del criminal al desplegar una conducta, ayudando a establecer mediante juicios de valor atenuantes o agravantes del delito.

3.2.5.1.3. Culpa.

La culpa, *lato sensu*, es la realización de un hecho ilícito que pudo evitarse, sin embargo, la ausencia de precaución o falta de intención en la conducta, deriva en la comisión del delito.

“Existe culpa, cuando se produce un resultado típicamente antijurídico por falta de previsión del deber de conocer, no solo cuando ha faltado al autor la representación del resultado que sobrevendrá, sino también cuando la esperanza

de que no sobrevenga ha sido fundamento decisivo de las actividades del autor, que se producen sin querer el resultado antijurídico y sin ratificarlo."[32]

Las teorías que estudian a la culpabilidad se dividen de la siguiente manera:

1. De la previsibilidad.- Se fundamenta en un vicio de la voluntad que origina la falta de cálculo de los alcances posibles y pronosticables de una acción.

2. De la previsibilidad y evitabilidad.- Afirma que el hecho es predecible, adicionando el carácter de eludible para la actualización de la culpa.

3. Del defecto de la atención.- Su principio radica en el incumplimiento de un sujeto de un deber contenido en la legislación.

Los elementos de la culpa, se manifiestan en primer término en la conducta necesaria para la existencia del delito, ya sea una acción o una omisión, posteriormente que esta conducta sea ejercida sin los cuidados y prudencia contemplados por el Estado, seguido de que las consecuencias jurídicas generadas puedan predecirse y eludirse, asimismo, que el comportamiento sea tipificable, finalmente que exista un vínculo entre el hacer o no hacer y la consecuencia carente de intención.

Las formas de culpa, se conceptualizan de la manera siguiente: "Consciente (con previsión o con representación):- El agente prevé el posible resultado penalmente tipificado, pero no lo quiere; abriga la esperanza de que no se producirá.- Inconsciente (sin previsión o sin representación):- El agente no prevé la posibilidad de que emerja el resultado típico, a pesar de ser previsible. No prevé lo

[32] Ibidem, p. 247.

que debió haber previsto. Según la mayor o menor facilidad de prever se clasifica en lata, leve y levísima.”[33]

Se puede ejemplificar la culpa consciente, cuando un individuo sabe que los frenos de su automóvil tienen un defecto en su funcionamiento, no obstante el pleno conocimiento de esta circunstancia, maneja el vehículo a una velocidad excesiva, esperando que ninguna persona transite por las calles que recorrerá. En esta conducta se aprecia la previsión de un hecho constitutivo de delito, pues existe la posibilidad de ocasionar daños y lesiones a otros conductores o transeúntes, sin embargo, con la esperanza de que no se verifique un siniestro el sujeto despliega su comportamiento.

Como ejemplo de culpa inconsciente, se establece un escenario en que una persona, limpia un revólver ante otra y sin calcular las consecuencias posibles de su conducta, acciona el mecanismo de disparo, lesionando a su acompañante. El hecho era pronosticable, pues es del conocimiento general la magnitud de la peligrosidad que implica el manipular un arma de fuego, sin embargo, el sujeto actuó sin los cuidados necesarios para evitar un accidente letal.

3.2.5.2. Culpabilidad en el delito informático.

Al examinar los preceptos que regulan los delitos informáticos en el *Código Penal del estado de Veracruz* y el *Código Penal Federal*, se encuentran distintos elementos que determinan la especie de culpabilidad inmersa en la descripción típica de la conducta antijurídica realizada.

[33]Op. Cit. Nota 5, p 251.

El artículo 181 de la legislación estatal veracruzana, es genérico en cuanto a la culpabilidad descrita en el tipo penal, pues no aparece ningún elemento que determine dolo o culpa en la conducta.

En su primer párrafo existen elementos normativos antijurídicos como los enunciados sin derecho y con perjuicio de tercero, los cuales carecen de un valor doloso o culposo, pues se pueden realizar con o sin conocimiento de las consecuencias jurídicas que conllevan. La falta de autorización o el menoscabo de un derecho no definen la intención del sujeto al realizar la conducta.

De la misma forma, la frase a ingresar en una base de datos, sistema o red de computadoras no presupone características de dolo o culpa, pues es una acción que evidentemente necesita la voluntad del agente, sin embargo, este personaje puede estar consciente de que su ingreso tiene resultados dañinos (dolo) o también es posible la falta de percepción del perjuicio de su comportamiento (culpa).

Con los elementos objetivos que continúan en la descripción del tipo penal informático en Veracruz, se le puede atribuir el carácter tanto doloso como culposo a la conducta, en los verbos obtener, conocer, utilizar, alterar o reproducir la información y en los vocablos intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático, es posible la manifestación de la culpa, pues no es necesario tener el conocimiento de que se está generando un menoscabo jurídico para que se configure el ilícito.

En el último párrafo del artículo que nos ocupa, es evidente la presencia de un elemento subjetivo doloso, pues la expresión *con fines de lucro* declara la inminencia de una total comprensión e intención del sujeto al realizar la conducta contraria a Derecho.

Para una mejor comprensión de las líneas anteriores, a continuación se exponen los siguientes ejemplos:

Delito informático culposo.- Un alumno de la clase de computación, no puede imprimir un documento y el maestro no se encuentra dentro del salón de clases, por tanto, sin estar autorizado, entra al sistema de conexión de hardware con la finalidad de arreglar su problema de impresión, esperando que su intromisión no sea descubierta, sin embargo, por la falta de conocimientos técnicos origina un daño irreversible a los controladores de las impresoras ocasionando un perjuicio a la institución educativa a la que pertenece.

En esta situación se observa, la culpa consciente ya que el alumno sabe que su conducta es carente de Derecho al no existir consentimiento de su maestro, no obstante lo anterior tiene la esperanza de no ser sorprendido en el despliegue de su acción, pero al carecer de la capacidad para manipular los sistemas informáticos, destruye los soportes lógicos de las impresoras provocando un deterioro en los derechos de un tercero, en este caso la escuela.

Delito informático doloso.- un hacker que carece de derecho para adentrarse virtualmente en un sistema computacional, interfiere un programa de banca electrónica, consiguiendo las claves interbancarias de las cuentas de ahorro e inversión de una persona física, para realizar transferencias monetarias para beneficio económico y personal.

En este escenario de acuerdo a la concepción doctrinal del dolo, se nota la presencia de un dolo directo, pues el resultado de la acción del sujeto evidentemente coincide con el propósito de lucro y lesión que tiene en su mente; dolo determinado porque la conducta se dirige hacia la delincuencia informática; inicial, debido a que su intención existe desde que emprende su comportamiento; dolo especifico, pues la voluntad agresiva del agente se encamina al bien jurídico

de la información; dolo simple, porque se allega de los instrumentos y medios tecnológicos necesarios para perpetrar el ilícito y dolo de daño, debido a que el resultado de la acción es la vulneración del bien protegido de la intimidad de la información.

3.2.5.3. Inculpabilidad.

La inculpabilidad es el aspecto negativo y la falta de culpabilidad, se materializa cuando al ejecutar un acto ilícito coinciden motivos concretos ajenos a la conciencia y libre albedrio del agente del delito.

"La inculpabilidad opera al hallarse ausentes los elementos esenciales de la culpabilidad: conocimiento y voluntad. Tampoco será culpable una conducta si falta alguno de los otros elementos del delito, o la imputabilidad del sujeto, porque si el delito integra un todo, sólo existirá mediante la conjugación de los caracteres constitutivos de su esencia."[34]

"El inculpable es completamente capaz y si no le es reprochada su conducta es porque, a causa de error o por no poder exigírsele otro modo de obrar, en el juicio de culpabilidad se le absuelve. Mas para todas las otras acciones su capacidad es plena."[35]

La inculpabilidad se traduce en la inexistencia de un vínculo de motivación corporal y mental del sujeto activo con la conducta que realiza.

---

[34]Op. Cit. Nota 5, p 257.
[35] Op. Cit. Nota 8, p 259.

3.2.5.3.1. Causas de inculpabilidad.

Las circunstancias extrañas a la capacidad de conocer y querer que concurren en la ejecución de un hecho realizado por sujeto imputable dando lugar a la inculpabilidad, son el error y la no exigibilidad de otra conducta.

3.2.5.3.2. Error.

Es un vicio psicológico que deriva en un conocimiento incorrecto de la verdad, se interpreta como la falsa apreciación de la realidad. Se clasifica en:

a. Error de derecho.- cuando un individuo al perpetrar un delito desconoce que su comportamiento está penado, este tipo de error no exime al agente de su responsabilidad pues la ignorancia de la ley no justifica su violación.

b. Error de hecho.- subdividido en:

i. Error esencial.- “el sujeto realiza una conducta antijurídica, pensando que es jurídica.”[36]

ii. Error accidental.- error en el golpe, cuando el resultado no es el deseado pero de la misma magnitud; error en la persona, radica en la confusión del objeto material del delito; error de delito, se realiza un ilícito diverso al pretendido.

Contemporáneamente ha surgido la clasificación del error de acuerdo a los elementos que constituyen la tipificación penal (error de tipo) o atendiendo a la licitud en la realización del hecho (error de prohibición).

[36] Op. Cit. Nota 3, p 239.

- Error de tipo.- la equivocación en el comportamiento recae en un vicio en el conocimiento de algún componente de la descripción penal del delito.

- Error de prohibición.- comprende el error invencible por estimarse que el hecho típico ejecutado no está prohibido; error invencible al considerarse que el hecho, en general prohibido, en el caso particular se encuentra justificado a virtud de una circunstancia que en realidad no tiene esa eficacia y el error invencible por creerse que el hecho, si bien prohibido, en el caso se halla amparado por una causa de justificación.

3.2.5.3.2. No exigibilidad de otra conducta.

"Con la frase no exigibilidad de otra conducta, se da a entender que la realización de un hecho penalmente tipificado, obedece a una situación especialísima, apremiante, que hace excusable este comportamiento."[37]

Es decir, es el inevitable comportamiento contrario a Derecho de un sujeto, realizado en un escenario determinado al carecer de opciones lícitas para actuar, eximiéndolo de su castigo al comprender las razones propias de la naturaleza humana que validan socialmente su actuación.

La naturaleza jurídica de esta excluyente de responsabilidad, es indeterminada y por tanto criticada por algunos juristas, pues no se ha podido señalar con precisión cuál de los dos elementos de la culpabilidad se anula cuando se manifiesta, no obstante lo anterior, las legislaciones penales la han incluido en sus apartados, delimitándola a través de las siguientes figuras:

[37] Op. Cit. Nota 5, p 270.

- El temor fundado.- Se trata de una coacción moral, circunstancias objetivas ciertas que obligan al sujeto a actuar de determinada manera.

- Estado de necesidad tratándose de bienes de la misma entidad.- El proceder de quien priva de un derecho para salvar otro de la misma importancia, no es constitutiva de delito, pues el Estado no puede exigir al sujeto, otro modo de actuar.

Las causas de inculpabilidad están previstas en el artículo 26 del *Código Penal del estado de Veracruz*, que es del tenor siguiente:

"Artículo 26.-Son causas de inculpabilidad:- I. Que razonablemente no pueda exigirse al agente una conducta diversa de la que llevó a cabo;- II. Que el agente actúe por miedo o temor fundado e irresistible de un mal inminente o grave en su persona o de alguien ligado a él por vínculos de parentesco, por lazos de amor o de estrecha amistad;- III. Que el agente realice la acción o la omisión bajo un error invencible sobre:- a) Alguno de los elementos objetivos que integran el tipo penal; o- b) La ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma o porque crea que está justificada su conducta.- Si el error es vencible, será responsable a título de culpa si el tipo legal admite ésta."

3.2.5.4. Causas de inculpabilidad en el delito informático.

Para que el sujeto activo del delito que conduce sus acciones a lesionar el bien protegido de la intimidad de la información, sea absuelto de las responsabilidades penales a las que es acreedor, es necesario que se hallen ausentes el conocimiento de la antijuricidad de su conducta y la voluntad plena de

realizarla, con las omisiones de estos elementos operará la inculpabilidad y el agente de delito informático no podrá ser sancionado.

Ahora bien, en los delitos informáticos considerados en el *Código Penal Federal* y en el *Código Penal para el estado de Veracruz*, por su naturaleza tienen cabida causas de inculpabilidad para que la persona que los cometa sea exculpada de su castigo, debido a que no es irreal que una persona piense que tiene la autorización para ingresar a una base de datos, por ejemplo, una secretaria que ingresa a la computadora de su jefe convencida de que tiene su consentimiento por la relación de confianza existente y como consecuencia, llega a conocer información confidencial contenida en dicho ordenador, realizando esta conducta con la idea errónea de que está legitimada para desplegar su conducta, asumiendo que su actuar es lícito y que no está quebrantando ninguna norma penal.

En esta situación se encuentra un error de tipo, pues existe un vicio de conocimiento de uno de los elementos de la tipificación de delito informático que influye directamente en la antijuricidad de la conducta, en particular la falta de derecho para ingresar a un sistema computacional.

Asimismo, cabe la posibilidad de que un individuo con conocimientos técnicos avanzados en informática, sea amenazado de muerte por parte de sicarios integrantes de la delincuencia organizada y sea obligado para que sin autorización alguna y perjudicando a una empresa que se negó a pagar un derecho de piso, destruya los soportes lógicos de facturación electrónica de esta persona moral, realizando esta conducta ilícita en contra de su voluntad.

En el ejemplo anterior, se observa el temor fundado como causa de inculpabilidad porque el sujeto activo del delito está actuando en respuesta al

terror producido por la intimidación de un tercero, que pone en riesgo apremiante un bien jurídico fundamental que es la vida.

3.2.6. Punibilidad y excusas absolutorias.

"Es la amenaza de una pena que establece la ley, para en su caso ser impuesta por el órgano jurisdiccional, de acreditarse la comisión de un delito. Cuando se habla de punibilidad se está dentro de la función legislativa."[38]

Las razones que el legislador estableció para que un ilícito no sea penado, a pesar de integrarse totalmente, constituyen las excusas absolutorias.

3.2.6.1. Punibilidad.

"La punibilidad es un elemento secundario del delito, que consiste en el merecimiento de una pena, en función o por razón de la comisión de un delito; dichas penas se encuentran establecidas en nuestro Código Penal."[39]

Una conducta será punible en el momento en que se vuelve digna de ser castigada con la penalidad establecida en la legislación punitiva válida y vigente, esta se concibe con el apercibimiento de sanción contenido en la ley para los ciudadanos que la transgreden.

En resumen, punibilidad es: "a) Merecimiento de penas; b) Conminación estatal de imposición de sanciones si se llenan los presupuestos legales; y, c) Aplicación fáctica de las penas señaladas en la ley."[40]

---

[38] Op. Cit. Nota 18, p 101.
[39] Op. Cit. Nota 3, p 263.

3.2.6.2. Punibilidad en los delitos informáticos.

Las penas contenidas en los tipos penales de delitos informáticos del orden federal son contenidas en el artículo 211 bis 1, para quien modifique, destruya o provoque pérdida de información de seis meses a dos años de prisión y de cien a trescientos días multa; y a quien conozca o copie información, de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Por otra parte, de acuerdo al artículo 211 bis 2, al ser sujeto pasivo el Estado, se aumenta la sanción a la persona que modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de la nación de uno a cuatro años de prisión y de doscientos a seiscientos días multa; al que conozca o copie información en igualdad de términos se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa, de la misma manera se agrava la penalidad de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal cuando la información derive de una institución de seguridad pública.

Asimismo, el numeral 211 bis 3, sanciona a la persona que estando autorizada para acceder a sistemas informáticos del Estado, indebidamente modifica, destruye o provoca pérdida de información contenida en los mismos, imponiéndole de dos a ocho años de prisión y de trescientos a novecientos días multa; en su segundo párrafo dispone que aquel que con las mismas características indebidamente copie información se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa, aumentando la pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal, cuando se trata de medios de almacenamiento informáticos en materia de seguridad pública.

---

[40] Op. Cit. Nota 8, p 275.

Los artículos 211 bis 4 y bis 5, contemplan como sujeto pasivo a las instituciones que integran el sistema financiero y castigan las mismas conductas realizadas en contra del Estado, estableciendo las siguientes penalidades: seis meses a cuatro años de prisión y de cien a seiscientos días multa, tres meses a dos años de prisión y de cincuenta a trescientos días multa, seis meses a cuatro años de prisión y de cien a seiscientos días multa, tres meses a dos años de prisión y de cincuenta a trescientos días multa, asimismo, considera que las penas previstas se incrementarán en una mitad cuando el comportamiento sea realizado por funcionarios o empleados de las instituciones que integran el sistema financiero.

El Artículo 211 bis 7 establece que las penas previstas en el capítulo de Acceso ilícito a sistemas y equipos de informática, se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

La sanción para los delitos informáticos dentro la codificación penal veracruzana, está comprendida en su artículo 181, que establece una pena de seis meses a dos años de prisión y multa hasta de trescientos días de salario a quien sin derecho y en perjuicio de un tercero, ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información en ellos contenida, o intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red, incrementando en una mitad esta condena cuando se despliegue la conducta con fines de lucro.

En ese tenor, es evidente que la novedosa creación de los delitos informáticos y la errónea idea de que los medios necesarios para su comisión están reservados para una mínima parte de la población, son aspectos que influyen directamente en la decisión del legislador veracruzano de establecer penas mínimas para su castigo, haciendo notar que los integrantes de la

legislatura federal se limitaron a establecer penas significativas únicamente cuando las victimas del ilícito son el Estado, la seguridad pública o las instituciones que integran el Sistema Financiero; sin embargo, es puntual precisar que actualmente la magnitud de los daños económicos que generan en el país estas conductas es preocupante, de acuerdo al Reporte Norton 2013 realizado por la empresa de seguridad informática *Symantec*. México ocupa el tercer lugar a nivel global de países en los que adultos que se han visto afectados por el cibercrimen alguna vez en su vida, generando un costo anual aproximado de $3,000.000 (USD), esta información se corrobora con el estudio *Hábitos de los Usuarios de Internet en México* 2013 sustentado por la *Asociación Mexicana de Internet*, que refleja la cantidad de usuarios de *Internet* en el país que se eleva aproximadamente a 45,100,000 de mexicanos, todos ellos potenciales víctimas de delitos informáticos, por tanto, tomando en consideración que la población total de México es de 112,336,538 de habitantes según el Censo de Población y Vivienda de 2010 elaborado por el *Instituto Nacional de Estadística y Geografía*, se calcula que alrededor de 40.15% del total de la población mexicana es susceptible de convertirse en sujeto pasivo del crimen informático.

Por los motivos y cifras anteriormente expuestas, los castigos incluidos en el artículo 181 del Código Penal para el Estado Libre y Soberano de Veracruz y en los numerales 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4, 211 bis 5, 211 bis 6 y 211 bis 7 del Código Penal Federal, evidentemente no guardan proporción con la dimensión de los menoscabos jurídicos realizables con los delitos informáticos.

3.2.6.3. Excusas absolutorias.

"Son aquellas causas que dejando subsistente el carácter delictivo de la conducta o hecho, impiden la aplicación de la pena."[41]

Se trata de comportamientos específicos que el Estado no castiga, por cuestiones de integridad moral, de acuerdo a una estrategia de combate al delito que las justifique sin excesos.

Cuando se está en presencia de una excusa absolutoria no se alteran la conducta, tipicidad, antijuricidad y culpabilidad de la acción, sin embargo, la probabilidad de su castigo queda eliminada.

Entre las excusas absolutorias se encuentran las siguientes:

- Excusa en razón de mínima temibilidad.- "Se manifiesta cuando el infractor cubre la totalidad de los daños y perjuicios ocasionados, antes de que la autoridad tome conocimiento del cometido delito sin violencia. "La razón de esta excusa debe buscarse en que la restitución espontánea es una muestra objetiva del arrepentimiento y de la mínima temibilidad del agente."[42]

- Excusa en razón de la maternidad consciente.- Aparece cuando el aborto es causado por un descuido de la madre o su embarazo deviene de una violación.

- Otras excusas por inexigibilidad.- Dentro de estas conductas se observa el encubrimiento de parientes y allegados, a través de acciones como el ocultamiento del propio agente criminal, la omisión de auxilio para investigar

[41] Ibidem, p 280.
[42] Idem.

delitos o perseguir familiares delincuentes, así como favorecer sin violencia su evasión.

- Excusa por graves consecuencias sufridas.- “Capta los casos en los cuales el sujeto activo sufre daños graves en su persona, de tal manera que sea hasta inhumana la imposición de una pena, o innecesaria, tratándose de personas de avanzada edad o precaria salud.”[43]

3.2.6.4. Excusas absolutorias en el delito informático.

En el despliegue de las conductas antijurídicas, típicas y culpables que están establecidas en el artículo 181 del *Código Penal para el estado de Veracruz* y 211 bis 1 al 211 bis 7 del *Código Penal Federal*, es posible encontrar algunas de las excusas absolutorias, en este caso del delito informático contemplado por dichos preceptos legales.

En primer lugar, estableciendo un contexto en que opere la excusa absolutoria en razón de mínima temibilidad del sujeto activo del ilícito informático, es factible considerar que al ocasionar un menoscabo sin derecho a un tercero mediante el ingreso a una base de datos o sistema de computadoras y alterar la información contenida en los mismos, al percatarse de las consecuencias de lesión que generó, se arrepienta y pague la totalidad de los daños y perjuicios producidos al sujeto pasivo.

En segundo término, existe la probabilidad de que un individuo no coopere con la investigación relativa a la comisión de un ilícito informático previsto por los preceptos penales mencionados anteriormente y no auxilie a las autoridades correspondientes en la persecución del delincuente que sea su cónyuge,

[43] Ibidem, p 282.

concubinario, parientes colaterales por consanguinidad hasta el cuarto grado, afinidad o que tengan un vínculo con el criminal informático por amor, respeto, gratitud o estrecha amistad, apareciendo alguna de las circunstancias descritas, no será procedente aplicar las penas previstas en las fracciones III y IV del artículo 400 del *Código Penal Federal* relativas al encubrimiento; sin embargo, esta excusa absolutoria incluye a todos los delitos no solo a los informáticos.

CAPÍTULO IV
MARCO JURÍDICO NACIONAL DEL DELITO INFORMÁTICO

4.1. GENERALIDADES.

México como país está conformado en una federación a la que pertenecen entidades federativas con libertad y soberanía propias, las cuales cuentan con su respectivo Poder Ejecutivo en la figura del Gobernador, Poder Legislativo fundándose en el Congreso ocal y Poder Judicial depositado en el Tribunal Superior de Justicia y Consejo de la Judicatura Local.

El Congreso local de cada uno de los estados debe contemplar en la creación de leyes los valores particulares y necesidades sociales de los ciudadanos que habitan en la entidad federativa correspondiente, siempre respetando los límites de las facultades legislativas conferidas por la Constitución Política Mexicana, estando acorde con el contenido de la ley suprema.

En el ámbito legislativo penal, encontramos delitos del orden federal y delitos del orden común o estatal, teniendo como fundamento el artículo 73 de la Carta Magna, que determina la atribución de los Congresos Locales de crear leyes

penales que contengan figuras delictivas sobre las materias que no estén reservadas para la Federación, del siguiente texto:

“Artículo 73. El Congreso tiene facultad:…- XXI. Para expedir: …-b) La legislación que establezca los delitos y las faltas contra la Federación y las penas y sanciones que por ellos deban imponerse; así como legislar en materia de delincuencia organizada; Las autoridades federales podrán conocer de los delitos del fuero común, cuando éstos tengan conexidad con delitos federales o delitos contra periodistas, personas o instalaciones que afecten, limiten o menoscaben el derecho a la información o las libertades de expresión o imprenta. En las materias concurrentes previstas en esta Constitución, las leyes federales establecerán los supuestos en que las autoridades del fuero común podrán conocer y resolver sobre delitos federales.”

Lo anterior da lugar a la presunción de que algunas conductas ilícitas se encuentren reguladas paralelamente por la Federación y por los estados libres y soberanos, sin embargo, los tipos penales contenidos en ambas legislaciones guardan características que los diferencian entre sí, siendo los principales contrastes que los delitos federales buscan la protección de la Federación, aunado a que son sancionados por autoridades federales, por lo que la injerencia de las estados en su aplicación queda reservada únicamente en los supuestos de concurrencia establecidos en la legislación federal.

El indiscutible avance de la tecnología, genera múltiples maneras de perpetrar crímenes cibernéticos que ataquen a la confidencialidad e intimidad de los datos contenidos en sistemas informáticos, causando lesiones jurídicas y económicas de enorme magnitud.

Los delitos informáticos en el marco jurídico nacional se encuentran tipificados en el ordenamiento federal en los artículos del 211 bis1 al 211 bis 7, del

Código Penal Federal y en capítulos especiales de diversas legislaciones penales locales que estudiaremos en el presente capítulo.

En ese sentido, los delitos informáticos regulados por el *Código Penal Federal* son aplicables únicamente cuando se configura la competencia establecida en el artículo 104, fracción I, de la *Constitución Política Mexicana* y 50, fracción I, inciso a) al l) de la *Ley Orgánica del Poder Judicial de la Federación*, conforme a lo siguiente:

"Artículo 104.- Los Tribunales de la Federación conocerán: I. De los procedimientos relacionados con delitos del orden federal…"

"Artículo 50.- Los jueces federales penales conocerán:- I. De los delitos del orden federal.- Son delitos del orden federal:- a) Los previstos en las leyes federales y en los tratados internacionales. En el caso del Código Penal Federal, tendrán ese carácter los delitos a que se refieren los incisos b) a l) de esta fracción;- b) Los señalados en los artículos 2 a 5 del Código Penal;- c) Los cometidos en el extranjero por los agentes diplomáticos, personal oficial de las legaciones de la República y cónsules mexicanos;- d) Los cometidos en las embajadas y legaciones extranjeras;- e) Aquellos en que la Federación sea sujeto pasivo;- f) Los cometidos por un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas;- g) Los cometidos en contra de un servidor público o empleado federal, en ejercicio de sus funciones o con motivo de ellas, así como los cometidos contra el Presidente de la República, los secretarios del despacho, el Procurador General de la República, los diputados y senadores al Congreso de la Unión, los ministros, magistrados y jueces del Poder Judicial Federal, los miembros de Consejo de la Judicatura Federal, los magistrados del Tribunal Electoral del Poder Judicial de la Federación, los miembros del Consejo General del Instituto Federal Electoral, el presidente de la Comisión Nacional de los Derechos Humanos, los directores o miembros de las Juntas de Gobierno o

sus equivalentes de los organismos descentralizados;- h) Los perpetrados con motivo del funcionamiento de un servicio público federal, aunque dicho servicio esté descentralizado o concesionado;- i) Los perpetrados en contra del funcionamiento de un servicio público federal o en menoscabo de los bienes afectados a la satisfacción de dicho servicio, aunque éste se encuentre descentralizado o concesionado;- j) Todos aquéllos que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la Federación;- k) Los señalados en el artículo 389 del Código Penal cuando se prometa o se proporcione un trabajo en dependencia, organismo descentralizado o empresa de participación estatal del Gobierno Federal;- l) Los cometidos por o en contra de funcionarios electorales federales o de funcionarios partidistas en los términos de la fracción II del artículo 401 del Código Penal."

Con base en lo anterior, se afirma que los ciudadanos en situaciones ajenas a los incisos del *Código Penal Federal* detallados anteriormente, encuentran protección al bien jurídico tutelado de la información solo por las leyes del fuero común.

4.2. MARCO JURÍDICO DE LOS DELITOS INFORMÁTICOS EN EL FUERO COMÚN.

Como ya se estableció, existen en el mundo del Derecho Penal delitos computacionales y delitos informáticos.

Los primeros son comportamientos delictivos realizados mediante el uso de tecnologías de la información que daña bienes jurídicos protegidos por otros tipos penales como el patrimonio y la seguridad sexual utilizando únicamente las redes cibernéticas como medio de comisión.

Los mencionados en segundo lugar son delitos que atacan propiamente bienes informáticos, no como medio sino como fin, cuya conducta no encuadra en los tipos penales convencionales, pues la afectación del bien jurídico de la información trasciende a todo el proceso de almacenamiento, tratamiento y transmisión de datos.

Dicho lo anterior, se procede a analizar los artículos del ordenamiento jurídico nacional que tipifican a los delitos informáticos en sí mismos.

4.2.1. Código Penal para el estado de Aguascalientes.

La legislación punitiva del estado de Aguascalientes, reformada por última ocasión el diecinueve de febrero de dos mil catorce, tipifica a los delitos informáticos en su capítulo XII relativo a los *Tipos Penales Protectores de la Confidencialidad y la Intimidad de la Información*, establecidos en el numeral 181, del tenor siguiente:

“ARTÍCULO 181.- Acceso informático indebido. El Acceso Informático Indebido consiste en:- I. Acceder a la información contenida en un aparato para el procesamiento de datos o cualquier dispositivo de almacenamiento de información sin autorización de su propietario o poseedor legítimo; o- II. Interferir el buen funcionamiento de un sistema operativo, programa de computadora, base de datos o cualquier archivo informático, sin autorización de su propietario o poseedor legítimo. Al responsable del Acceso Informático Indebido se le aplicará de 1 a 3 meses de prisión, de 150 a 300 días multa así como el pago de la reparación de los daños y perjuicios ocasionados. Si quien realiza el Acceso Informático Indebido es el responsable del mantenimiento o seguridad del sistema de información sobre el que se perpetra, se le aplicará de 2 a 6 meses de prisión, de 300 a 600 días multa así como el pago de la reparación de daños y perjuicios ocasionados.”

4.2.2. Código Penal para el estado de Baja California.

La legislación penal del estado de Baja California, es vanguardista en la tipificación de delitos informáticos, pues incorpora el veinte de abril de dos mil doce, la suplantación de identidad al *Título Tercero relativo a los Delitos contra la Inviolabilidad del Secreto y de los Sistemas y Equipos de Cómputo y Protección de Datos Personales*, regulando atinadamente una conducta que se manifiesta principalmente a través de los medios informáticos, quedando incluidas las conductas ilícitas informáticas en los siguientes artículos:

“Artículo 175 Bis.- A quien sin autorización o indebidamente, 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 multa equivalente de cien a trescientos días.”

“Artículo 175 Ter.- A quien sin autorización o indebidamente, copie o accese a 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 multa equivalente de cincuenta a ciento cincuenta días de salario mínimo vigente”

“Artículo 175 Quater.- Agravación de la pena.- Las penas previstas en los artículos anteriores se duplicarán cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del Estado o Municipios.- Sin perjuicio de la agravación de la pena, que se imponga conforme al párrafo anterior, la pena se aumentará hasta en una mitad más, cuando el delito se ejecute por un servidor público.”

“Artículo 175 Quinquies.- Tipo y punibilidad.- Al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad, se

le impondrá pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días multa.- Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien además se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito así como en el supuesto de que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines.- Serán equiparables al delito de usurpación o suplantación de identidad y se impondrán las penas establecidas por este artículo, cuando se actualicen las siguientes conductas:- I.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido o genere un daño patrimonial para sí o para otro valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;- II.- Al que transfiera, posea o utilice datos identificativos de otra persona con la intensión de cometer, intentar o favorecer cualquier actividad ilícita, y- III.- Al que asuma, suplante o se apropie o utilice a través del *Internet*, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.”

4.2.3. Código Penal para el estado de Chiapas.

La ley punitiva de la entidad federativa chiapaneca, fue reformada por última ocasión el uno de mayo de dos mil trece, en su Título Décimo Noveno se observan los *Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática*, advirtiéndose el Acceso Ilícito a Sistemas de Informática en el Capítulo II de dicho apartado, en donde se hace distinción cuando las conductas afectan a una entidad pública protegida, a una persona física o moral y estableciendo que dichos ilícitos serán perseguidos por querella, quedando regulados de la forma siguiente:

“Artículo 439.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.- Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentará en una mitad.”

“Artículo 440.- Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.”

“Artículo 441.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.”

“Artículo 442.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa.”

“Artículo 443.- Los delitos previstos en este título serán sancionados por querella de parte ofendida.”

4.2.4. Código Penal del estado de Chihuahua.

Por otra parte, el estado de Chihuahua amplía la protección a sus habitantes de los ilícitos informáticos, contemplándolos en la ley sustantiva penal vigente a partir del dieciocho de diciembre de dos mil trece, dentro del Título Vigésimo Segundo que contiene los *Delitos Contra la Seguridad y el Normal Funcionamiento de las Vías de Comunicación y de los Medios de Transporte, Capítulo IV relativo al Uso y Acceso Ilícito a los Sistemas y Equipos Informáticos y de Comunicación*, adicionando el diecinueve de noviembre de dos mil once, los delitos informáticos en los siguientes preceptos:

“Artículo 327 Bis.- A quien sin la debida autorización o excediendo la que tenga y con ánimo de lucro, en beneficio propio o de un tercero, acceda, copie, modifique, destruya, deteriore, intercepte, interfiera, o use, información contenida en equipos informáticos o de comunicación, se le impondrán de seis meses a tres años de prisión y de cien a cuatrocientos días multa.”

“Artículo 327 Ter.- Al que diseñe, programe, fabrique, introduzca, importe, comercialice o distribuya programas de cómputo, aparatos, sistemas, códigos de acceso, o cualquier dispositivo físico, que tengan por objeto violar uno o más mecanismos de seguridad de equipos informáticos, de comunicación, de programas de cómputo, en beneficio propio o de un tercero, se le impondrán de seis meses a cuatro años de prisión y de doscientos a quinientos días multa.”

“Artículo 327 Quater.- Al que valiéndose de equipos informáticos o de comunicación, utilice indebidamente, datos o información personal de otro para ostentarse como tal sin consentimiento de éste, ya sea en beneficio propio o de un tercero, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.”

“Artículo 327 Quinquies.- Las penas previstas en este Capítulo se incrementarán en una mitad cuando las conductas sean cometidas en contra de una entidad pública estatal o municipal.”

4.2.5. Código Penal del estado de Coahuila de Zaragoza.

Este ordenamiento penal adecuó el primero de septiembre de dos mil seis, su contenido conforme a la tecnología contemporánea, castigando en su Capítulo Tercero los *Delitos contra la Seguridad en los Medios Informáticos*, haciendo una diferencia cuando estas conductas causan daño a particulares o entidades públicas, asimismo, se encuentran asentadas en artículos separados las circunstancias agravantes de dichos ilícitos, catalogándolos de la siguiente forma:

“Artículo 281 Bis. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de particulares. Se aplicará prisión de tres meses a tres años y multa a quien:- l. Sin autorización para acceder a un sistema informático y con perjuicio de otro, conozca, copie, imprima, use, revele, transmita, o se apodere de datos o información reservados, contenidos en el mismo.- II. Con autorización para acceder a un sistema informático y con perjuicio de otro, obtenga, sustraiga, divulgue o se apropie de datos o información reservados en él contenidos.- Si la conducta que en uno u otro caso se realiza es con el ánimo de alterar, dañar, borrar, destruir o de cualquier otra manera provocar la pérdida de datos o información contenidos en el sistema, la sanción será de cuatro meses a cuatro años de prisión y multa.”

“Artículo 281 Bis 1. Circunstancias agravantes de los delitos anteriores.- Las penas previstas en el artículo anterior, se incrementarán en una mitad más:- I. Si el agente actuó con fines de lucro.- II. Si el agente accedió al sistema informático

valiéndose de información privilegiada que le fue confiada en razón de su empleo o cargo, o como responsable de su custodia, seguridad o mantenimiento.”

“Artículo 281 Bis 2. Sanciones y figuras típicas de los delitos contra la seguridad en los medios informáticos cometidos en perjuicio de una entidad pública. Se aplicará prisión de seis meses a seis años y multa a quien:- I. Sin autorización, acceda, por cualquier medio a un sistema informático, de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, para conocer, copiar, imprimir, usar, revelar, transmitir o apropiarse de sus datos o información propios o relacionados con la institución.- II. Con autorización para acceder al sistema informático de una entidad pública de las mencionadas en el párrafo segundo del artículo 194, indebidamente copie, transmita, imprima, obtenga, sustraiga, utilice divulgue o se apropie de datos o información propios o relacionados con la institución.- Si la conducta que en uno u otro caso se realiza, tiene la intención dolosa de alterar, dañar, borrar, destruir, o de cualquier otra forma provocar la pérdida de los datos o información contenidos en el sistema informático de la entidad pública, la sanción será de uno a ocho años de prisión y multa.- Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.”

“Artículo 281 Bis 3. Circunstancias agravantes en los delitos anteriores. Las penas previstas en el artículo anterior se incrementarán en una mitad más:- I. Si el agente obró valiéndose de alguna de las circunstancias agravantes previstas en el artículo 290 Bis 1.- II. Si el hecho constitutivo de delito fue cometido contra un dato o sistemas informáticos concernientes al régimen financiero de las entidades públicas que se mencionan en el artículo 194, o por funcionarios o empleados que estén a su servicio.- III. Si la conducta afectó un sistema o dato referente a la salud o seguridad pública o a la prestación de cualquier otro servicio público.”

Asimismo, el legislador coahuilense fue oportuno y atinado al establecer en un precepto adicional las definiciones de los conceptos de informática que incluyó en los tipos penales descritos, para una mayor comprensión jurídica por parte de los gobernados, autoridades jurisdiccionales y ministeriales, quedando asentados estos conceptos en el artículo 281 bis 4, que a continuación se transcribe.

“Artículo 281 Bis 4. Norma complementaria en orden a la terminología propia de los delitos contra la seguridad de los medios informáticos. A los fines del presente Capítulo, se entiende por:- I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.- II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.”

4.2.6. Código Penal para el estado de Colima.

El tres de mayo de dos mil ocho fue publicado en el periódico oficial del estado de Colima la adición del artículo 240 bis al Código Penal de dicha entidad federativa, que contempla el delito informático dentro de los delitos patrimoniales de esta forma:

“Artículo 240 Bis.- Se le impondrá una pena de seis meses a seis años de prisión y multa de trescientos a mil unidades al que de manera dolosa y sin derecho alguno, ni autorización de quien pueda otorgarlo conforme a la Ley, utilice o tenga acceso a una base de datos, sistemas o red de computadoras o a cualquier parte de la misma, con el firme propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información en perjuicio de otro.-

De igual forma, la misma sanción del párrafo anterior se impondrá a quien 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.- Si el sujeto activo es empleado o dependiente del ofendido, la pena corporal aumentará de cuatro años seis meses, la mínima, y de trece años seis meses la máxima."

Por otro lado, incluido entre los delitos contra el patrimonio, en dicha legislación penal se advierte el fraude, equiparando este ilícito en el artículo 233, fracción VII (incorporada el nueve de mayo de dos mil nueve), con una conducta que se considera como ilícita informática puesto que atenta fundamentalmente contra la confidencialidad de la información contenida en un sistema o medio cibernético, inclusive el legislador agrega una agravante cuando el comportamiento es desplegado por un individuo con estudios superiores en informática, por lo que se estima que esta fracción debe estar regulada en el capítulo correspondiente a los delitos informáticos, a continuación se transcribe el precepto mencionado para ilustrarlo con precisión.

"Artículo 232.- Al que engañando a alguien o aprovechándose del error en que éste se halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido se le impondrá prisión de seis meses a ocho años y multa hasta por 85 unidades."

"Artículo 233.- Se equipara al fraude y se sancionará con las penas previstas en el artículo anterior al que:… VII.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo

cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido.- En el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, la pena se aumentará hasta en cuatro años más, y en caso de reincidencia hasta cinco años más de prisión."

4.2.7. Código Penal del estado de Guanajuato.

El estado de Guanajuato brinda una protección deficiente a sus habitantes respecto de los delitos informáticos, pues dichos comportamientos carecen de legislación penal que los contemple efectivamente, debido a que el código penal correspondiente se limita a integrarlos dentro del capítulo relativo a la *Violación de Correspondencia*, dando lugar a la tipificación del delito informático en la fracción II del artículo 231 de la ley penal sustantiva, de texto siguiente:

"Artículo 231.- Se aplicará de seis meses a tres años de prisión y de cinco a treinta días multa, a quien indebidamente:…II.- Accese, destruya o altere la comunicación o información contenida en equipos de cómputo o sus accesorios u otros análogos.- No se impondrá pena alguna a quienes ejerciendo la patria potestad o la tutela, ejecuten cualquiera de las conductas antes descritas, tratándose de sus hijos menores de edad o de quienes se hallen bajo su guarda.- Se requerirá querella de parte ofendida cuando se trate de ascendientes y descendientes, cónyuges o concubinos, parientes civiles o hermanos."

4.2.8. Código Penal para el Estado Libre y Soberano de Jalisco.

La legislación penal jalisciense guarda similitud con la del estado de Baja California, por lo que respecta a los delitos informáticos, pues se advierte del contenido de su Título Sexto que regula la *Revelación de Secretos y la Obtención ilícita de información*, que mediante decreto publicado el doce de noviembre de dos mil trece, se incluyeron acertadamente en el artículo 143 Quáter el delito de suplantación de identidad dentro del capítulo IV de ese apartado, estipulando agravantes cuando el sujeto activo cuente con una licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática.

De igual manera, mediante la reforma realizada el veintitrés de agosto de dos mil doce, los legisladores del estado de Jalisco incorporaron en el capítulo III contenido en el Título Sexto del código penal mencionado, el comportamiento antijurídico que ejecuta una persona después de apropiarse indebidamente de información.

A continuación se realiza la transcripción de los preceptos legales del ordenamiento punitivo jalisciense que regulan las conductas delictivas informáticas.

“Artículo 143 Bis.- Al que sin autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa.- Las penas previstas en este artículo se incrementarán en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.”

“Artículo 143 Ter.- Se impondrán de tres a seis años de prisión a la persona que, teniendo acceso a bases de datos con información confidencial de instituciones o personas, emplee esta información para fines ilícitos, o trasmita esta información a terceros para ser empleada con fines ilícitos.”

“Artículo 143 Quáter.- Comete el delito de suplantación de identidad quien suplante con fines ilícitos o de lucro, se atribuya la identidad de otra persona por cualquier medio, u otorgue su 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 salarios.- Serán equiparables al delito de suplantación de identidad y se impondrán las penas establecidas en este artículo:- I. Al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido para sí o para otro o genere un daño patrimonial a otro, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;- II. Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, favorecer o intentar cualquier actividad ilícita; o- III. Al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona.- Se aumentará hasta en una mitad las penas previstas en el presente artículo, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito; así como en el supuesto en que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática.”

4.2.9. Código Penal para el estado de Morelos.

Los comportamientos ilícitos informáticos, fueron adicionados el veinte de octubre de dos mil diez, al Título Cuarto del Código Penal para el estado de Morelos que garantiza la protección de los ciudadanos de habitan dicho territorio contra conductas antijurídicas bajo el rubro de *Delitos Contra la Libertad y otras Garantías*, para quedar asentados en el Capítulo VIII, de la forma que a continuación se transcribe:

“Artículo 148 Quárter.- Comete el 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;- 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;- III. Haga uso de la red de Internet utilizando cualquier medio para realizar actos en contra de las personas o cosas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para perturbar la paz pública o que atente contra el orden constitucional; y- IV. 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.”

La codificación criminal del estado de Morelos, en la parte relativa a la regulación de los delitos informáticos es similar a la observada en las entidades federativas de Colima, Veracruz y Sinaloa, sin embargo, se distingue de estas pues agrega una tipificación que castiga la utilización del *Internet* para perturbar la paz pública, conducta que puede ser considerada como terrorismo cibernético.

4.2.10. Código Penal para el estado de Nuevo León.

La codificación penal de Nuevo León, sufrió su última reforma publicándose en el periódico oficial de dicho estado, el seis de enero de dos mil catorce, cuenta con una singular regulación de los delitos informáticos, pues únicamente los adecua en aquellos ilícitos contra el sistema de justicia, teniendo como sujeto pasivo a alguna institución de seguridad pública o procuración de justicia que se encuentre protegida por algún medio de seguridad, tipificándolos de la siguiente forma:

“Artículo 225 Bis 1.- A quien indebidamente conozca, obtenga, copie o utilice información contenida en cualquier sistema informático de alguna institución de seguridad pública o procuración de justicia, protegido por algún medio de seguridad, se le impondrá pena de cinco a diez años de prisión y multa de quinientas a mil cuotas. Si el responsable es o hubiera sido servidor público, se impondrá además, inhabilitación de cinco a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.”

“Artículo 225 Bis 2.- A quien esté autorizado para acceder a sistemas y equipos de informática de alguna institución de seguridad pública o procuración de justicia, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cinco a diez años de prisión y multa de quinientas a mil cuotas. Si el responsable es o hubiera sido servidor público, se impondrá además, una mitad más de la pena impuesta e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”

“Artículo 226.- Las disposiciones anteriores se aplicaran también a todos los funcionarios o empleados de la administración pública, cuando en el ejercicio de su cargo ejecuten los hechos o incurran en las omisiones expresadas en los propios artículos.”

4.2.11. Código Penal del Estado Libre y Soberano de Puebla.

La entidad federativa poblana, tuvo el pasado treinta de enero de dos mil trece una importante reforma en su Código Penal, específicamente en los delitos informáticos pues se adicionó un apartado completo de estas conductas que da origen al Capítulo Vigésimo Quinto, del tenor siguiente:

“Artículo 475.- Se impondrá prisión de uno a cinco años, multa de cincuenta a quinientos días de salario 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.”

“Artículo 476.- 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 de 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 de multa.”

“Artículo 477.- 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 dos años de prisión y de doscientos a seiscientos días de multa.”

“Artículo 478.- 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 cuatro años de prisión y de trescientos a novecientos días de 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 dos años de prisión y de ciento cincuenta a cuatrocientos cincuenta días de 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 dos a cinco años de prisión y multa de quinientos a mil días de salario mínimo general vigente. 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."

4.2.12. Código Penal para el estado de Querétaro.

El Título Séptimo de esta codificación penal, contempla los *Delitos contra la Inviolabilidad del Secreto y el Acceso Ilícito a Sistemas de Informática*, observándose con plenitud los delitos informáticos en los numerales 159 Ter y 159 Quater, agregados a ley penal queretana el veintidós de abril de dos mil once, estando tipificados de la forma siguiente:

"Artículo 159 Ter.- Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema 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 o no por algún sistema de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.- Las penas señaladas en el párrafo anterior se aplicarán a aquellos

que teniendo autorización para ingresar al sistema informático, hagan uso indebido de la información, para sí o para otro.”

“Artículo 159 Quater.- Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos del Estado, protegidos o no por algún sistema 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 o no por algún medio 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 o no por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a setecientos cincuenta días multa. 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 cualquier empleo, puesto, cargo o comisión de carácter público.”

4.2.13. Código Penal para el Estado Libre y Soberano de Quintana Roo.

Las características del delito informático, como el menoscabo al bien jurídico protegido de la confidencialidad de la información contenida en alguna base de datos, tiene una relación directa con el de delito de usurpación de identidad recién agregado a la ley penal quintanarroense el seis de septiembre de dos mil trece, sobre todo en la fracción IV del Artículo 195 Septies, pues encuadra el delito informático conocido como *phishing*, descrito como a continuación se asienta:

“Artículo 195-Sexties (sic). El delito de usurpación se define como al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro la identidad de una persona o otorgue consentimiento para llegar (sic) a cabo la usurpación o suplantación de su identidad, se le impondrá una pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días de multa.”

“Artículo 195-Septies. Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el artículo 195-Sexties a quienes:…IV. Al que por algún uso del medio informático, telemático o electrónico, o use la red de *Internet* montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecta la confiabilidad y variación de la navegación de la red para obtener lucro indebido.- En el supuesto que el activo tenga licenciatura, ingeniería o cualquier grado académico reconocido en los rubros mencionados, la pena se aumentará hasta en una mitad más.”

4.2.14. Código Penal para el estado de Sinaloa.

El estado de Sinaloa fue la primera entidad federativa en legislar en materia de delitos informáticos, la regulación de estos ilícitos se realizó en el año mil novecientos noventa y dos, por tal razón, fueron incluidos erróneamente en el apartado de delitos contra el patrimonio, describiendo las conductas típicas informáticas de la siguiente manera:

“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.”

4.2.15. Código Penal para el estado de Tabasco.

La ley punitiva del estado de Tabasco, si bien tipificó los delitos informáticos hace aproximadamente doce años desde su reforma de veintitrés de noviembre de dos mil dos, los legisladores tabasqueños realizaron una adecuada separación y conceptualización de estas conductas, pues las incluyeron en el Titulo Decimotercero Bis correspondiente a *Delitos contra la Seguridad en los Medios Informáticos y Magnéticos*, catalogándolos en acceso sin autorización, daño informático y falsificación informática, tipificando estas conductos como se observa a continuación:

“Artículo 326 bis.- Al que intercepte, interfiera, reciba, use o ingrese por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal, o a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos, se le impondrá de seis meses a dos años de prisión y de cincuenta a ciento cincuenta días multa.”

“Artículo 326 bis 1.- A quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible

contenido en computadoras personales, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético, se le sancionará con penas de dos a ocho años de prisión y de cuatrocientos a mil doscientos días multa.- Cuando el activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más."

"Artículo 326 bis 2.- Se impondrán penas de dos a seis años de prisión y de cuatrocientos a mil días multa, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal o en un sistema de redes de computadoras, base de datos, soporte lógico, siempre que para ello se requiera autorización y no la obtenga.- Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este Título."

"Artículo 326 bis 3.- Cuando los ilícitos previstos en este Título se cometan utilizando el equipo de cómputo de terceras personas, las penas se incrementarán en una mitad."

4.2.16. Código Penal para el estado de Tamaulipas.

El ordenamiento penal tamaulipeco, contiene una regulación especial de los *Delitos de Revelación de Secretos y de Acceso Ilícito a Sistemas y Equipos de Informática*, dentro de su Título Séptimo, el cual fue adicionado en los artículos que lo integran el veinticinco de diciembre de dos mil uno, los cuales protegen la confidencialidad de la información en sus artículos 207 bis al 207 Sexties, estableciendo expresamente que su persecución será por querella de parte agraviada, en los preceptos que se transcriben en las líneas siguientes:

“Artículo 207-Bis.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo de seguridad o que no tenga derecho de acceso a el, se le impondrá una sanción de uno a cuatro años de prisión y multa de cuarenta a ochenta días salario.”

“Artículo 207 Ter.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a seis años de prisión y multa de doscientos a seiscientos días salario.”

“Artículo 207 Quater.- Al que sin autorización conozca o copié información contenida en sistemas o equipos de informática de alguna dependencia pública, protegida por algún mecanismo se le impondrá una sanción de dos a cinco años de prisión y multa de cien a trescientos días salario.”

“Artículo 207 Quinquies.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente modifique, destruye o provoque pérdida de información que contengan se impondrá una sanción de tres a ocho años de prisión y multa de trescientos a ochocientos días salario.”

“Artículo 207 Sexies.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, indebidamente copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y multa de cien a trescientos días salario.- Los delitos previstos en este título serán sancionados por querella de la parte ofendida.”

4.2.17. Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave.

Los delitos informáticos contemplados en el ordenamiento penal veracruzano que constituyen la base del presente estudio, se encuentran regulados en el Título IV del código penal mencionado, el cual corresponde a los *Delitos Contra la Intimidad Personal y la Inviolabilidad del Secreto*, dando lugar al Capítulo III en el que se incluyen en su artículo 181, del tenor siguiente:

"Artículo 181.- Comete delito informático quien, sin derecho y con perjuicio de tercero:- I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o- II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.- Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad."

Cabe precisar que la tipificación de las conductas ilícitas informáticas en Veracruz, guarda similitud con la redacción del Códigos Penales para los estados de Sinaloa, Aguascalientes, Tabasco, Morelos y Colima, ordenamientos jurídicos que carecen de reformas por más de una década en materia de cibercriminalidad, por tal motivo, es importante, que sean actualizados a la realidad contemporánea como el caso de los Códigos Penales de Baja California, Puebla y Jalisco, entidades federativas que han sabido responder a sus habitantes otorgándoles una certidumbre jurídica en la protección de sus derechos de informáticos.

4.2.18. Código Penal para el estado de Zacatecas.

Los crímenes informáticos están incluidos en el título séptimo de la codificación penal zacatecana, apartado que en su capítulo II protege la seguridad en los medios informáticos y magnéticos, el cual fue añadido el cuatro de agosto de dos mil doce, quedando descritos los tipos penales informáticos de la forma siguiente:

“Artículo 192 Bis.- Se impondrá de seis meses a dos años de prisión y multa de cincuenta a ciento cincuenta cuotas, al que ingrese o use por cualquier medio sin la autorización debida o, excediendo la que tenga, a una computadora personal o dispositivo electrónico, a un sistema de red de computadoras, un soporte lógico de programas de cómputo o base de datos.”

“Artículo 192 Ter.- Se impondrá de dos a ocho años de prisión y multa de ciento cincuenta a trescientas cuotas, a quien sin autorización modifique, destruya o deteriore en forma parcial o total, archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras personales, dispositivos electrónicos, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético.- Cuando el sujeto activo tenga el carácter de encargado del manejo, administración o mantenimiento de los bienes informáticos dañados, las penas se incrementarán en una mitad más.”

“Artículo 192 Quater.- Se impondrá de dos a seis años de prisión y multa de doscientas a trescientas cuotas, al que copie o imite los originales de cualquier dato, archivo o elemento intangible contenido en una computadora personal, dispositivo electrónico, en un sistema de redes de computadoras, base de datos o soporte lógico, siempre que para ello se requiera autorización y no la obtenga.- Las mismas sanciones se aplicarán al que utilice o aproveche en cualquier forma, los bienes informáticos falsificados, previstos en este Capítulo.”

“Artículo 192 Quintus.- Cuando los ilícitos previstos en este Capítulo se cometan por servidores públicos o ex servidores públicos dentro del año siguiente al término de su función, en perjuicio de los archivos, bases de datos o cualquier otro elemento intangible contenido en computadoras, dispositivos electrónicos, sistemas o redes de cómputo, soportes lógicos, o cualquier otro medio magnético propiedad o al servicio del Estado o los Municipios, se impondrá una mitad más de la pena y destitución a los primeros e inhabilitación a ambos, por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”

“Artículo 192 Sextus.- Las penas señaladas en este Capítulo se aumentarán en dos terceras partes de la pena impuesta, cuando las conductas previstas en el mismo se realicen para cometer un delito; o cuando la información obtenida se utilice en provecho propio o ajeno; y se aplicarán, en su caso, las reglas del concurso.- Los delitos previstos en este Capítulo se perseguirán a petición de parte.”

4.3. MARCO JURIDICO DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL FEDERAL.

Los delitos informáticos comprendidos en la legislación sustantiva penal de la Federación, han sido materia de estudio a lo largo del capítulo anterior de este trabajo referente a la teoría del delito informático, por ese motivo, abordaremos su contenido desde la perspectiva del *Proyecto de Decreto que Reforma y Adiciona diversas disposiciones al Código Penal Federal, en materia de Delitos en contra de Medios o Sistemas Informáticos*, presentado el quince de febrero de dos mil doce, por la Comisión de Justicia de la Cámara de Diputados,

publicado en la Gaceta Parlamentaria, año XV, número 3480-III, realizando un cuadro comparativo respecto del Código Penal Federal vigente.

Texto Vigente	Propuesta de reforma
Titulo Noveno	Titulo Noveno
Revelación de secretos y acceso ilícito a sistemas y equipos de informática	Revelación de secretos y acceso ilícito a sistemas y equipos de informática
Capítulo I	Capítulo I
Revelación de secretos	Revelación de secretos
Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.	Artículo 211 Bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. Se impondrán las mismas penas que refiere el párrafo anterior a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad.
Capítulo II	Capítulo II
Acceso ilícito a sistemas y equipos de informática	Acceso ilícito a sistemas y equipos de informática
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	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.	mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Se aplicará una pena de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización y con el ánimo de causar un daño, acceda y modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática que no estén protegidos por algún mecanismo de seguridad. En los casos en que el daño provocado por el acceso o la modificación no autorizados obstaculice o disminuya la capacidad de funcionamiento del sistema o equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes. 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 seis meses a dos años de prisión y de cien a trescientos días multa. La pena aplicable será de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa al que sin autorización conozca o copie información contenida en sistemas o equipos de informática no protegidos por algún mecanismo de seguridad.
Artículo 211 Bis 2. Al que sin autorización modifique, destruya o	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.	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.	Al que sin autorización y con el ánimo de causar un daño, 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.	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 o también sin autorización acceda a dichos equipos o medios o mediante cualquier mecanismo les cause un daño, 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. En los casos en que el daño provocado por el acceso o la modificación no autorizados, obstaculice o disminuya la capacidad de funcionamiento del sistema o

	equipo informático las penas previstas en los párrafos anteriores se incrementarán hasta en dos terceras partes.
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 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. Las penas establecidas en los párrafos anteriores se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero, las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo primero del artículo 400 Bis de este ordenamiento.
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,	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.	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 o divulgue información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días de multa. Las penas previstas en este artículo se incrementan al doble cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. Las penas establecidas en los párrafos primero y segundo de este artículo se incrementarán hasta en dos terceras partes y se impondrán sin perjuicio de las que resulten aplicables por la comisión de otros delitos al que realice, para beneficio propio o de cualquier tercero; las conductas que describen los párrafos anteriores con la finalidad de realizar o encubrir las operaciones con recursos de procedencia ilícita a que se refiere el párrafo segundo del artículo 400 Bis de este ordenamiento.

La aprobación del proyecto de decreto de reforma y adición presentado por la *Comisión de Justicia de la Cámara de Diputados*, actualiza los tipos penales

de delitos informáticos comprendidos en el *Código Penal Federal*, al incorporar en el artículo 211 bis, la penalización y castigo de propagación y uso indebido de mensajes de texto, imágenes, archivos de voz y conversaciones que no sean obtenidos mediante intervención judicial de comunicaciones privadas, es decir, castigará a aquellas personas que sin un mandamiento fundado y motivado expedido por una autoridad jurisdiccional, violenten sistemas y equipos informáticos a través del uso de dispositivos ya sea fijos o móviles con la finalidad de allegarse de información ajena y difundirla, inclusive a través de la suplantación de identidad.

Por otro lado, la reforma al artículo 211 bis 1, acertadamente hace extensiva la protección a equipos y redes informáticas que carecen de un sistema de seguridad con el afán de resguardar la información de las pequeñas y medianas empresas del país que muchas veces no cuentan con la infraestructura necesaria para protegerla, sin embargo, las penas de prisión y multa se mantienen idénticas a las del texto vigente, las cuales son bajas si se considera el valor económico de la información de las personas morales.

De la misma manera, las adecuaciones realizadas al numeral 211 bis 2, que corresponden a los delitos informáticos en los que el sujeto pasivo es el Estado mexicano, no varían en lo relativo a su punibilidad, por lo que se consideran penas que no guardan proporción con la magnitud del perjuicio que pudieran sufrir las entidades gubernamentales que manejan datos confidenciales como es el *Instituto Federal de Acceso a la Información y Protección de Datos o la Comisión Federal de Telecomunicaciones*.

Asimismo, la adición del último párrafo a los preceptos 211 bis 4 y 211 bis 5, es un gran avance en el combate del lavado de dinero, pues llena una laguna jurídica que existía, ya que no se encontraba tipificado el blanqueamiento de capitales ilícitos a través de transferencias electrónicas de valores a cuentas

bancarias que se ubican en paraísos fiscales, que son aprovechados por los cibercriminales al ser difíciles de rastrear debido al secreto bancario.

CAPÍTULO V
PROPUESTAS

5.1. PANORAMA ACTUAL DE LOS DELITOS INFORMÁTICOS EN EL ESTADO DE VERACRUZ.

El radical avance tecnológico en los últimos años ha marcado un cambio sustancial en el acontecer diario de los habitantes del estado de Veracruz, pues la manera de relacionarse entre sí y con su entorno, a través del uso de herramientas informáticas, como computadoras personales y celulares inteligentes, generan un beneficio evidente en ámbitos sociales, económicos y productivos.

De acuerdo a cifras presentadas en el año dos mil trece por la *Asociación Mexicana de Internet* en su *Noveno Estudio sobre los Hábitos de los internautas en México*, en el año dos mil seis, 20.2 millones de personas utilizaban *Internet* en el país, elevándose el número de usuarios a 45.1 millones para el año de dos mil doce, siendo impresionante la magnitud y velocidad de la tasa de crecimiento del acceso a *Internet* de 223.26% en tan solo seis años, que se traduce en un

incremento de 24.9 millones de navegantes de *Internet* en México en ese periodo.

Entre las bondades tecnológicas figuran las redes sociales, que son un espacio virtual que permite ejercer libremente la libertad de expresión con la facilidad de capturar ideas mediante un teclado y accionar un botón para publicarlas en la web, actividad que constituye el 82% de las realizadas por el internauta mexicano, también las aplicaciones de mensajería instantánea, las cuales conectan a miles de usuarios que coinciden en tenerlas instaladas en sus respectivos dispositivos informáticos y habilitan una comunicación inmediata, así como la facultad de compartir imágenes, textos, videos, entre otros archivos electrónicos, hábito acostumbrado por el 61% de los usuarios de *Internet* en el país, asimismo, la forma de realizar operaciones financieras cotidianas ha evolucionado gracias a la invención de la banca electrónica, que otorga a quienes son afectos a utilizarla, la capacidad para transferir capitales económicos a través de un sistema informático, transacciones monetarias que representan el 33% de las actividades en línea en México.

Debido a las anteriores demostraciones de progreso en la tecnología, la calidad de vida de los individuos y la prosperidad de las empresas aumenta considerablemente, pues incentivan su desarrollo y competitividad, ya que los beneficios tecnológicos aportados facilitan la interacción e intercambio de información, pues de acuerdo a los resultados arrojados en dos mil doce por la *Encuesta en Hogares sobre Disponibilidad y Uso de las Tecnologías de la Información* realizada por el *Instituto Nacional de Estadística y Geografía*, el principal uso que se da a la computadora es para realizar labores escolares (52.3%), seguido de actividades vinculadas con la comunicación (48.6%), cifras que corroboran lo significativo del acceso a *Internet* en materia educativa y laboral.

No obstante todos los beneficios que representan los avances en tecnologías de la información, es un hecho que estos también propician el

surgimiento de novedosos fenómenos delictivos, al aumentar el campo de acción de los criminales que buscan diversificar la manera de transgredir derechos y cometer ilícitos, a través de los delitos informáticos con un crecimiento preocupante.

El informe de la *Secretaría de Seguridad Pública* emitido con motivo del *Quinto Informe de Gobierno* refiere que la policía cibernética manifiesta que de septiembre de 2010 a julio de 2011 se atendieron 5 mil 582 denuncias ciudadanas en materia de delitos cibernéticos.

Sin embargo, los criminales han encontrado un nicho de impunidad al castigo de sus conductas antijurídicas en la delincuencia informática, al carecer en el Estado de Veracruz de una legislación eficaz y actualizada que proteja los bienes informáticos, acorde con la tendencia evolutiva de su comisión.

La protección jurídica de los bienes informáticos es un verdadero reto para el poder legislativo veracruzano, pues tomando en consideración los números de la *Encuesta en Hogares sobre Disponibilidad y Uso de las Tecnologías de la Información* de dos mil once y el *Censo de Población y Vivienda* de dos mil diez, ambos elaborados por el *Instituto Nacional de Estadística y Geografía*, indican que el 25.4% por ciento de los habitantes del estado de Veracruz son usuarios de *Internet* y la población veracruzana asciende a 7,643,194 (siete millones seiscientos cuarenta y tres mil ciento noventa y cuatro), por tanto, se concluye que aproximadamente 1,941,371 (un millón novecientos cuarenta y un mil trescientos setenta y uno) ciudadanos que residen en el territorio veracruzano son potenciales víctimas de un delito informático y por ende es necesaria la actualización del *Código Penal del Estado* para fortalecer el marco jurídico punitivo en materia de ilícitos de la información.

Una legislación penal sustantiva renovada adecuadamente es el punto de partida para proteger los bienes jurídicos informáticos de la población veracruzana, pues desde la inclusión de los delitos de este tipo al *Código Penal para el Estado Libre y Soberano de Veracruz*, en el año dos mil cuatro los legisladores del estado han sido omisos en responder al desarrollo tecnológico por lo que la eficacia de la disposición penal vigente está en duda, ante la velocidad del desarrollo actual de la informática de acuerdo a las cifras expresadas en los párrafos anteriores.

La aparición de nuevas conductas antijurídicas que vulneran bienes informáticos que carecen de protección legal es una amenaza jurídica latente para los veracruzanos, pues es evidente el rezago legislativo al no reconocer los diputados locales la necesidad de modernizar la tipificación de estos comportamientos ilícitos, lo cual es apremiante y un gran desafío para la legislatura estatal, ante el abuso realizado por los delincuentes informáticos, que aprovechan las lagunas jurídicas existentes permitiendo la impunidad de sus acciones.

La adecuación del código penal veracruzano en materia de delitos informáticos debe comenzar percibiendo la realidad contemporánea que permea en el estado, identificando las formas actuales en las que se lesionan los bienes que tutelan la información, puesto que los adelantos de la tecnología han rebasado a la legislación penal actual.

Las modificaciones legislativas en Veracruz necesitan atender los espacios jurídicos vacíos en la respectiva codificación referente a los delitos informáticos, es factible determinar estas lagunas comparando el contenido del texto vigente con los diversos códigos penales de distintas entidades federativas que se han reformado recientemente en materia informática (Baja California, Jalisco y Puebla).

Asimismo, la redacción de los preceptos tiene que derivar en un catálogo que perfeccione los tipos de delitos informáticos, sustentado en instrumentos legales de vanguardia en el tema como el *Convenio sobre la Ciberdelincuencia en Europa*, conocido informalmente como el *Convenio de Budapest*.

La protección de los bienes jurídicos informáticos en Veracruz, es necesaria pues resulta indispensable para el correcto desarrollo de la sociedad, ya que el crecimiento del uso cotidiano de las redes y sistemas informáticos está directamente vinculado con el progreso de la entidad federativa, en diversos ámbitos sociales y económicos, por ejemplo, en la educación básica es casi forzoso el uso de una computadora para realizar tareas y trabajos y en el sector empresarial para llevar inventarios de mercancías, plataformas de presupuestos y registros de egresos, por mencionar algunos aspectos de la vida diaria que se ven afectadas por la delincuencia informática.

En ese tenor, los funcionarios del Poder Judicial del estado de Veracruz han expresado su sentir respecto de los delitos informáticos, en dos mil once Raúl Pimentel Murrieta, magistrado del *Tribunal Superior de Justicia del Estado*, manifestó a la prensa que: “el Código Penal del Estado de Veracruz está rezagado para combatir delitos informáticos, ya que la evolución tecnológica supera al ordenamiento jurídico.”[44]

De igual manera, en agosto de dos mil trece, Arturo Montes de Oca en su carácter de Director del *Centro de Control, Comando, Comunicaciones y Cómputo (C-4)* dependiente de la *Secretaría de Seguridad Pública del estado de Veracruz*, declaró a los medios que: “es alta la incidencia de los llamados delitos cibernéticos pero mucha gente no los denuncia o reporta como tales, porque los desconocen admitiendo que urge tipificarlos en el *Código Penal* para perseguirlos e identificar a

[44] http://www.alcalorpolitico.com/informacion/codigo-penal-del-estado-de-veracruz-rezagado-para-combatir-delitos-informaticos-magistrado-del-tsje-80536.html, 11 de marzo de 2014.

los responsables”[45], asimismo, mencionó que al día se reciben en la dependencia a su cargo cuarenta llamadas relacionadas con este tipo de delitos; sin embargo, si no existe sustento como autoridad, el principio jurídico dice que lo que no está prohibido está permitido, revelando que en la entidad federativa se han identificado delitos de ese tipo como los fraudes electrónicos donde se pide a las personas a través de un mail, que depositen alguna cantidad de dinero para recibir un premio, así como secuestros exprés, pidiendo alguna transferencia electrónica, fraude electrónico y otros.

De las anteriores declaraciones de autoridades judiciales y administrativas en materia de seguridad pública, se pone en evidencia la simbólica protección de los bienes jurídicos informáticos en el Estado y el claro problema de vulnerabilidad social derivado del uso perjudicial de las tecnologías de la información por la falta de un régimen jurídico completo que garantice la tutela eficaz de los derechos en materia de información.

Por otro lado, para efectos de comprender apropiadamente el contenido del texto del artículo 181 del *Código Penal para el estado de Veracruz*, referente a los delitos informáticos se procede a transcribir el precepto:

“Artículo 181.-Comete delito informático quien, sin derecho y con perjuicio de tercero:- I. Ingrese en una base de datos, sistema o red de computadoras para obtener, conocer, utilizar, alterar o reproducir la información, en ellos contenida; o - II. Intercepte, interfiera, use, altere, dañe o destruya un soporte lógico o programa informático o la información contenida en el mismo o en la base, sistema o red.- Al responsable de este delito se le impondrán de seis meses a dos años de prisión y multa hasta de trescientos días de salario. Si se cometiere con fines de lucro las penas se incrementarán en una mitad.”

[45] http://www.imagendelgolfo.com.mx/resumen.php?id=405477, 11 de marzo de 2014.

Del análisis del tipo penal del delito informático que se encuentra en la legislación penal veracruzana, se aprecian diversas carencias jurídicas que no permiten proteger correctamente a los ciudadanos de los novedosos comportamientos delictivos que lesionan bienes informáticos.

En primer lugar, el artículo establece elementos normativos del tipo penal en los enunciados *sin derecho* y *con perjuicio de tercero*, frases que si bien contienen una valoración legal del comportamiento presumiendo su antijuricidad, constituyen una limitante para encuadrar la conducta y por ende, la ausencia de estos elementos deriva invariablemente en atipicidad por falta de integración del tipo penal generando la no existencia del hecho delictivo.

Lo anterior, si se toma en consideración, que muchas ocasiones las personas si tienen derecho a ingresar en una base de datos, sistema o red de computadoras y esta circunstancia no significa que estén exentos de causar un menoscabo jurídico a los bienes informáticos contenidos en los sistemas a los cuales tienen pleno acceso.

Igualmente, es prudente delimitar quiénes son los terceros que pueden verse afectados por el despliegue de la conducta, pues en ningún momento se menciona una protección al propio estado de Veracruz, como entidad federativa y a los municipio que la integran, ya que también son potenciales víctimas de delitos informáticos.

Por otra parte, en la definición de delito informático que nos ocupa aparecen elementos de valoración cultural del tipo penal muy importantes que no corresponden al lenguaje jurídico, sino al área de estudio de tecnologías de la información como las palabras sistema de computadoras, soporte lógico e información, por lo que vale la pena añadir un apartado en el que se conceptualicen adecuadamente estos términos, pues el juzgador necesita tenerlos

claros para emitir correctamente un juicio de valor cuando una causa penal formada con motivo de un delito informático este en sus manos, ya que el asimilar el significado de estos léxicos tecnológicos es fundamental para decidir si existe o no la conducta delictiva.

Una laguna jurídica de los delitos informáticos en Veracruz, radica en la falta de actualización ante las novedosas formas de perpetrar ilícitos que dañan bienes de la información, de acuerdo a lo declarado ante la prensa por Martín Gerardo Franco Sesma, Delegado Estatal de la *Comisión Nacional para la Defensa de los Usuarios de las Instituciones Financieras* en Veracruz, en el primer trimestre del presente año, la dependencia federal a su cargo ha registrado treinta y cuatro casos de suplantación de identidad, casi el doble de los registrados en el mismo periodo del dos mil trece, cuando se registraron diecinueve casos, estimando que de continuar con esta incidencia, en el estado se duplicarán los casos de este tipo registrados en el 2013, cuando tuvo 78 casos, asimismo, indicó que este comportamiento se presenta comúnmente en los bancos y tiendas departamentales que ofrecen créditos y suele darse de dos formas, la primera cuando son sustraídos los estados de cuenta de los buzones de las casas de los usuarios y la segunda cuando las personas llegan a módulos bancarios de plazas comerciales donde les ofrecen la oportunidad de obtener alguna tarjeta de crédito.

Aunado a lo anterior, el fenómeno delictivo robo de información personal de manera fraudulenta, mejor conocido como *phishing* está en considerable aumento en las redes sociales, pues se han convertido en una plataforma ideal para realizar ataques informáticos anónimamente haciéndose pasar los delincuentes por otras personas, enviando mensajes falsos con el fin de obtener un beneficio perjudicando a un tercero, de conformidad con el *Reporte de Cibercrimen de Norton* en el 2012 hubo únicamente en *Facebook* casi seis millones de fraudes manuales y cerca de 600 mil falsas ofertas y encuestas, por lo

que la inclusión de su castigo en el código penal veracruzano sería un acierto en la búsqueda de la renovación de los delitos informáticos en el estado.

Las estadísticas reflejan la magnitud del daño provocado por los delitos informáticos a los ciudadanos veracruzanos, por tanto, es necesario armonizar su punibilidad mínima con la proporción de las afectaciones económicas, patrimoniales y la inseguridad que propician, debiéndose incrementar las penas con la finalidad de disuadir su comisión y castigar estos ilícitos que generan un desfalco aproximado de $3,000.000 USD en el país, de acuerdo al *Reporte Norton 2013* realizado por la empresa de seguridad informática Symantec, México.

Las agravantes contempladas en el artículo 181 del Código Penal del estado de Veracruz, únicamente contemplan el hecho de que la información se utilice con fines de lucro, sin embargo, existen diferentes circunstancias que se pueden considerar para incrementar la punibilidad de los delitos informáticos, entre ellas que sean realizados en contra del Estado o los municipios, que la conducta sea desplegada por un servidor público, considerando también que el sujeto activo del delito cuente con estudios profesionales en materia de informática.

5.2. PROPUESTA DE REFORMA AL ARTÍCULO 181 DEL CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE VERACRUZ.

Debido a las deficiencias legislativas apuntadas y ante la magnitud del avance tecnológico que genera la necesidad apremiante de proteger a los veracruzanos de las nuevas formas de cometer delitos informáticos, se realiza la siguiente propuesta:

Artículo 181.- Se impondrán de dos a seis años de prisión y multa hasta de novecientos días de salario a los siguientes sujetos:

Al que sin autorización, por cualquier medio ingrese a sistemas informáticos, destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos protegidos o no por algún sistema de seguridad.

Al que sin autorización copie, transmita, imprima, obtenga, sustraiga, utilice divulgue o se apropie de información contenida en sistemas o equipos de informática protegidos o no por algún sistema de seguridad.

Al que revele, divulgue o utilice indebidamente o en perjuicio de otro, información, conversaciones o mensajes de texto, imágenes o archivos de voz, contenidos en sistemas o equipos informáticos, obtenidos a través de mecanismos distintos a la intervención de comunicación privada, mediante el empleo de aparatos o dispositivos electrónicos fijos o móviles o a través de la suplantación de identidad.

Las penas señaladas en el párrafo primero se aplicarán a aquellos que teniendo autorización para ingresar al sistema informático, hagan uso indebido de la información, para sí o para otro y se duplicarán cuando las conductas delictivas se ejecuten en contra de sistemas o equipos de informática del Estado de Veracruz o sus Municipios.

Si el sujeto activo del delito es servidor público, se le sancionará, además, con la destitución del empleo, cargo o comisión e inhabilitación para ejercer otro hasta por seis años.

Artículo 181 Bis.- A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento

informáticos de seguridad pública del Estado de Veracruz, protegido o no por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a setecientos cincuenta días multa. 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 cualquier empleo, puesto, cargo o comisión de carácter público.

Artículo 181 Ter.- Al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad, se le impondrá pena de cuatro a ocho años de prisión y de cuatrocientos a mil días multa.

Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien además se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito.

Serán equiparables al delito de usurpación o suplantación de identidad y se impondrán las penas establecidas por este artículo, cuando se actualicen las siguientes conductas:

I.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido o genere un daño patrimonial para sí o para otro valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;

II.- Al que transfiera, posea o utilice datos identificativos de otra persona con la intensión de cometer, intentar o favorecer cualquier actividad ilícita, y

III.- Al que asuma, suplante o se apropie o utilice a través del *Internet*, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.

Artículo 181 Quáter.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido para sí o para otro valiéndose de alguna manipulación informática, instrucciones de código, predicción, intercepción de datos de envío, reinyecte datos, use la red de redes montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados, imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecte la confiabilidad, y variación de la navegación en la red o use artificio semejante para obtener lucro indebido, se le impondrá pena de cuatro a ocho años de prisión y de cuatrocientos a mil días multa.

En el supuesto que el activo tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines, las penas previstas en este capítulo se aumentarán hasta en cuatro años más, y en caso de reincidencia hasta cinco años más de prisión.

Artículo 181 Quinquies. A los fines del presente capítulo, se entiende por:

I. Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos para generar, enviar, recibir, recuperar, procesar o almacenar información de cualquier forma o por cualquier medio.

II. Dato informático o información: toda representación de hechos, manifestaciones o conceptos, contenidos en un formato que puede ser tratado por un sistema informático.

La anterior propuesta de reforma al código penal veracruzano en materia de delitos informáticos se adecua a la realidad actual que prevalece en el estado, pues busca tipificar las nuevas conductas delictivas que implican un grave riesgo y vulnerabilidad para los bienes jurídicos informáticos de las personas, como lo son la suplantación de identidad y *phishing*.

De la misma manera, elimina elementos normativos del tipo penal innecesarios, permitiendo con esto que se integre debidamente la conducta antijurídica a la a su descripción concretada en la ley, quitando candados legales al combate de estos delitos a través de la legislación positiva.

Asimismo, incorpora mayores penas para un delincuente informático y contempla agravantes cuando el sujeto pasivo sea el estado de Veracruz o el Municipio, cuando se atente en contra de la seguridad pública estatal y, la más importante pues aplica para la totalidad de las víctimas es, cuando el criminal cuente con algún grado académico en informática o estudios afines.

El apartado complementario que describe la terminología relativa a las tecnologías de información establecidas al tipificar los delitos informáticos, es incluido con el afán de otorgar certidumbre jurídica a la población veracruzana, para evitar confusiones de conceptos al momento de que una autoridad ministerial o jurisdiccional emita la determinación correspondiente.

Los puntos anteriormente descritos son evidencia de la vanguardia jurídica que requiere la protección de los bienes jurídicos informáticos y por ese motivo la respuesta legislativa que se propone es inspirada en los diversos ordenamientos

penales nacionales de reciente modificación que se han preocupado por salvaguardar dichos bienes ante la irrupción de las nuevas tecnologías.

Los habitantes del estado de Veracruz merecen ser protegidos en sus bienes informáticos con efectividad, siendo la legislación el punto de partida de esa defensa jurídica.

CONCLUSIONES

PRIMERA. Al estudiar los diversos conceptos de delitos informáticos, se encuentran diversas acepciones y enfoques, distinguiéndolos de los conocidos como delitos cibernéticos, siendo el principal matiz, que los informáticos lesionan el bien jurídico propio de la información atentando en contra de su confidencialidad, mientras que los cibernéticos agreden bienes jurídicos que ya se encuentran protegidos en la legislación como el patrimonio.

Conocer las múltiples clasificaciones de delitos informáticos, permite percatarse de la gran variedad de maneras en las que se puede afectar la información de una persona y que no existe el único límite para los criminales informáticos sin escrúpulos es la velocidad del desarrollo de la tecnología.

SEGUNDA. Al haber analizado a la luz de la teoría del delito los artículos correspondientes a los ilícitos informáticos contemplados en el *Código Penal para el Estado Libre y Soberano de Veracruz* y *Código Penal Federal*, se fomentó el estudio de sus componentes jurídicos y se pudo establecer en qué casos se configura una conducta ilícita o esta no llega a constituirse cuando se atenta en contra de un bien informático.

Al aprender acerca de los elementos positivos y negativos del delito informático en Veracruz, se vislumbran las deficiencias en la tipificación básica de estas conductas, en comparación con la realizada en el orden federal que es más completa.

TERCERA. Familiarizarse con las diversas legislaciones del orden nacional que incorporan en sus textos a los delitos informáticos, es fundamental para observar que existen entidades federativas donde los legisladores se han preocupado por actualizar las leyes punitivas realizando las reformas necesarias para solventar la protección de los bienes informáticos de la población.

En contraste, en algunas legislaturas estatales se ha manifestado la indiferencia al desarrollo de nuevas tecnologías y la vanguardia en la forma de delinquir que traen aparejadas, pues ha sido omisa la adecuación de la ley penal a la realidad contemporánea, generando impunidad a las actuales conductas desplegadas por los delincuentes informáticos.

CUARTA. En Veracruz desde la inclusión, hace una década, de los delitos informáticos, no se ha respondido a la necesidad de proteger los bienes jurídicos informáticos de los habitantes del estado, de acuerdo a cifras basadas en estadísticas fundamentadas y respaldadas, en la entidad federativa es apremiante una modificación al código penal estatal que sea la base que permita una adecuada defensa de los derechos de la información de la población, ante el riesgo latente de su vulneración producto del veloz desarrollo de las tecnologías informáticas.

Ante esta exigencia legislativa, se propone una reforma al artículo 181 del *Código Penal para el Estado Libre y Soberano de Veracruz* en materia de delitos informáticos, que se ajusta al entorno real que predomina en el estado, tipificando nuevos comportamientos ilícitos, que elimine limitantes en su tipificación e

incremente las penas para su castigo contemplando agravantes necesarias para disuadir su comisión y confiriendo certidumbre jurídica al conceptualizar correctamente los términos tecnológicos.

BIBLIOGRAFÍA

Amuchategui Requena, Griselda Irma, DERECHO PENAL, 3ª ed, Editorial Oxford, México, 2005.

Cámpoli, Gabriel Andrés, DERECHO PENAL INFORMÁTICO EN MÉXICO, Editorial INACIPE, México, 2004.

Carrancá y Trujillo Raúl, Carrancá y Rivas Raúl, DERECHO PENAL MEXICANO (PARTE GENERAL), 23ª ed, Editorial Porrúa, México, 2007.

Castellanos Tena, Fernando, LINEAMIENTOS ELEMENTALES DE DERECHO PENAL, 46ª ed, Editorial Porrúa, México, 2005.

Jiménez de Asúa, Luis, LECCIONES DE DERECHO PENAL, Obra Compilada y Editada, Editorial Pedagógica Iberoamericana, México, 1995.

Jiménez de Asúa, Luis, LA LEY Y EL DELITO, 11ª ed, Editorial Sudamericana, Argentina, 1980.

López Betancourt, Eduardo, TEORÍA DEL DELITO, 15ª ed, Editorial Porrúa, México, 2008.

Plascencia Villanueva, Raúl, TEORÍA DEL DELITO, 3ª reimpresión, Instituto de Investigaciones Jurídicas, México, 2004.

Porte Petit Candaudap, Celestino, APUNTAMIENTOS DE LA PARTE GENERAL DEL DERECHO PENAL, 19ª ed, Editorial Porrúa, México, 2001.

Téllez Valdés, Julio, DERECHO INFORMÁTICO, 4ª ed, Editorial McGraw Hill, México, 2009.

LEGISGRAFÍA

Constitución Política de los Estados Unidos Mexicanos.

Código Penal Federal.

Ley Orgánica del Poder Judicial de la Federación.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Código Penal para el estado de Aguascalientes.

Código Penal para el estado de Baja California.

Código Penal para el estado de Chiapas.

Código Penal del estado de Chihuahua.

Código Penal del estado de Coahuila de Zaragoza.

Código Penal para el estado de Colima.

Código Penal del estado de Guanajuato.

Código Penal para el Estado Libre y Soberano de Jalisco.

Código Penal para el estado de Morelos.

Código Penal para el estado de Nuevo León.

Código Penal del Estado Libre y Soberano de Puebla.

Código Penal para el Estado Libre y Soberano de Quintana Roo.

Código Penal para el estado de Sinaloa.

Código Penal para el estado de Tabasco.

Código Penal para el estado de Tamaulipas.

Código Penal para el Estado Libre y Soberano de Veracruz de Ignacio de la Llave

Código Penal para el estado de Zacatecas.

LINKOGRAFÍA

http://es.wikipedia.org/wiki/Información

http://www.inegi.org.mx/est/contenidos/Proyectos/Encuestas/Hogares/modulos/endutih/endutih2013/default.aspx

http://www.larousse.com/es/diccionarios/ingles-espanol/hack/16335

http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=348&Type=1

http://www.inegi.org.mx/est/contenidos/proyectos/ccpv/cpv2010/Default.aspx

http://gaceta.diputados.gob.mx/Gaceta/61/2012/mar/20120328-III.html#DictamenaD2

http://www.alcalorpolitico.com/informacion/codigo-penal-del-estado-de-veracruz-rezagado-para-combatir-delitos-informaticos-magistrado-del-tsje-80536.html

http://www.imagendelgolfo.com.mx/resumen.php?id=405477

http://e-veracruz.mx/nota/2014-03-29/seguridad/robo-de-identidad-se-incrementa-al-doble-en-veracruz

http://www.cem.itesm.mx/derecho/referencia/diccionario/bodies/i.htm