UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

FACULTAD DE DERECHO

DIVISIÓN DE ESTUDIOS DE POSGRADO

"LOS DELITOS INFORMÁTICOS CONTENIDOS EN EL CÓDIGO PENAL FEDERAL, ASPECTOS TÉCNICOS DE LOS ELEMENTOS DEL TIPO PENAL Y UNA PROPUESTA FORENSE PARA SU PERSECUCIÓN EN INTERNET"

T E S I S

QUE PARA OBTENER EL GRADO DE ESPECIALIDAD EN DERECHO PENAL

P R E S E N T A :
LIC. ENRIQUE LÓPEZ CORDERO

TUTORA :
DRA. MARÍA TERESA AMBROSIO MORALES

CIUDAD UNIVERSITARIA **2017**

A mi amada esposa
María Concepción
Por su infinito apoyo
y enorme cariño,
eres una mujer excepcional

A mis estimados Maestros
Porque gracias a su gran
generosidad hacen que estudiar
derecho penal sea un privilegio

A mi querida Universidad, por
haberme cobijado en sus históricos
recintos y haber inculcado en mí,
ese espíritu puma, eternamente
agradecido

Un agradecimiento muy especial a
la Doctora María Teresa Ambrosio,
por su gran apoyo en la realización
de este trabajo de tesis, y por ser
una Profesionista comprometida
con un gran espíritu innovador tan
necesario para nuestro México

INDICE

INTRODUCCIÓN

El uso de las computadoras en el progreso mundial es enorme, a grado tal que se han convertido en herramientas necesarias y en la mayoría de las veces son indispensables para diversas actividades. Han tenido un impacto en la globalización y en la vida cotidiana, en la forma de hacer negocios, en la comunicación, en la educación, en realidad, en todo lo que representa la gestión de la información. Esta tecnología electrónica de alto nivel de procesamiento de datos, ha traído una suma de grandes beneficios, no obstante, esta evolución rápida y radical también ha planteado una serie de problemas, tanto de naturaleza socioeconómica, política y también de naturaleza jurídica, esto último, por la proliferación de conductas ilícitas que por su naturaleza sólo eran cometidas de forma material y no virtual, como el robo, el fraude, el acoso sexual, terrorismo, entre otras.

Es tan importante el tema de los delitos informáticos, que el Congreso de las Naciones Unidas sobre prevención del delito y justicia penal, celebrado en Brasil en Abril de 2010 en su 12ª Sesión, se trató de manera prioritaria el delito informático, esto por ocupar un lugar destacado al poner de relieve la gran importancia que sigue teniendo este tema y los serios retos que plantea. Estos congresos se han convertido a lo largo de 60 años en los foros internacionales más amplios y diversos para el intercambio de opiniones y experiencias en materia de investigación y elaboración de leyes, políticas y programas entre los Estados; asimismo, la Convención de Budapest sobre ciberdelincuencia ha representado el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos a través de Internet, elaborado por el Consejo de Europa en Estrasburgo, y cuyo objetivo principal es aplicar una política penal común encaminada a la protección de la sociedad contra la ciberdelincuencia, específicamente adoptando una legislación adecuada y el fomento de la cooperación internacional; tratado del que México ya forma parte desde 2014.

No obstante de que es posible realizar una descripción adecuada de los tipos de delitos informáticos encontrados en los tratados internacionales, difícilmente se

puede presentar una síntesis relacionada con el alcance de las pérdidas causadas por ellos y el número real de delitos cometidos, por su compleja forma de comisión.

Los objetivos de la presente tesis es, por un lado, entender el delito informático o como lo llaman los especialistas internacionales delito cibernético; describiendo la forma de participación del sujeto activo, los bienes jurídicos que las normas internacionales han definido y los medios para su comisión, así como el estudio interpretativo de los delitos informáticos que contempla el Código Penal Federal; por otro lado, desarrollar los aspectos importantes, tanto jurídicos como técnicos, para la investigación y persecución de estos delitos. Lo anterior para armonizar el marco jurídico contra las crecientes amenazas de la ciberdelincuencia en México.

Este trabajo de investigación está dividido en cinco capítulos donde y de una forma precisa, especifico los temas torales para comprender el delito informático, es por ello que en el primer capítulo se abordan los aspectos fundamentales de internet, desde su origen, hasta la manera en que los equipos de cómputo logran establecer una comunicación estructurada para transferir datos informáticos, establecidos en el modelo de siete capas OSI (Sistema Abierto de Interconexión por sus siglas en inglés), desarrollado por la Organización Internacional de Normalización ISO y el Protocolo TCP/IP de comunicación.

El segundo capítulo contiene los fundamentos constitucionales que regulan, en su parte dogmática, los derechos al acceso a las tecnologías de la información y a los servicios de telecomunicaciones; así como, las atribuciones del Ministerio Público y la policía para la investigación de delitos, la función y objetivos del Sistema Nacional de Seguridad Pública; además los fundamentos legales que regulan las conductas ilícitas en el contexto de los sistemas informáticos. Todo esto estructurado como el marco normativo que sustenta este trabajo de tesis.

El tercer capítulo, contiene de manera general los trece delitos informáticos más representativos, impactantes y recurrentes en el ámbito internacional, y que la misma Convención de Budapest tiene desarrollados como los que atentan contra

el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos que reafirman el derecho de todos a la libertad de expresión, de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad.

En el cuarto capítulo, realizo un estudio interpretativo del contenido del tipo penal, sobre delitos informáticos considerados por el legislador a través del Código Penal Federal; lo anterior, siguiendo la línea de análisis que han desarrollado catedráticos del Posgrado de la Facultad de Derecho de la UNAM, tanto en el aula como a través de la doctrina y de sus publicaciones. De ésta forma, analizo los elementos del tipo penal, tales como: la acción, el bien jurídico tutelado, la forma de participación del sujeto activo, las calidades específicas tanto del sujeto activo como del pasivo, el objeto material, los medios comisivos, las circunstancias de tiempo, modo, lugar y ocasión, los elementos normativos y el carácter doloso de la conducta, todos estos elementos para los delitos informáticos.

En el quinto capítulo, el cual es la base de mi propuesta de persecución de los delitos informáticos, en él abordo la técnica informática para rastrear los vestigios que dejan las conexiones ilícitas, lo cual realizo utilizando la herramienta informática wireshark y su descripción; asimismo, desde un enfoque del derecho comparado, propongo los tipos penales que, de manera especial, necesita el Código Federal Penal para ser apto en la persecución de estas conductas ilícitas.

Se utilizaron fuentes públicas, incluyendo el Convenio Sobre la Ciberdelincuencia de Budapest, 23.XI.2001; vigente para los Estados miembros del Consejo de Europa y los demás Estados signatarios, y del que el Estado Mexicano ya es parte desde 2014[1]; el cual fue anunciado por la subprocuradora Jurídica y de Asuntos Internacionales de la PGR, Mariana Benítez; así como, por el subsecretario para Asuntos Multilaterales y Derechos Humanos de la Secretaría de Relaciones Exteriores, Juan Manuel Gómez Robledo. Asimismo, se consultó el Estudio

[1]http://www.milenio.com/policia/Cibercriminalidad-Mexico-adhiere-Convenio_de_Budapest-PGR-delitos_informaticos-delitos_en_internet_0_274173006.html. Fecha de consulta 18 de Julio de 2017 20:30.

Integral sobre Delito Cibernético, Proyecto de febrero de 2013; de la Oficina de las Naciones Unidas para la Droga y el Delito con sede en Viena; ésta año con año, publica un informe que ofrece una visión general de la labor de la ONUDD en todo el mundo, para ayudar a los Estados Miembros a hacer frente a la amenaza que representan las drogas, la delincuencia y el terrorismo. Además de la publicación de la UIT sobre el delito cibernético: fenómenos, desafíos y respuesta legal que fue preparado por el Prof. Dr. Marco Gercke en septiembre de 2012, en virtud de que la UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (TIC); encargado de asignar espectro radioeléctrico mundial y órbitas de satélites, también desarrolla las normas técnicas que aseguran que las redes y las tecnologías se interconectan sin problemas en todo el mundo. Además de las disposiciones del Código Penal Federal, en el Capítulo II del Título Noveno, Libro Segundo intitulado como: Acceso ilícito a sistemas y equipos de informática; artículos 211 Bis 1; 211 Bis 2; 211 Bis 3; 211 Bis 4; 211 Bis 5; 211 Bis 6; 211 Bis 7, que entraron en vigor al día siguiente de la publicación en el Diario Oficial de la Federación de fecha 17 de mayo de 1999.

ABREVIATURAS

CPEUM	Constitución Política de los Estado Unidos Mexicanos
CNPP	Código Nacional de Procedimientos Penales
CPF	Código Penal Federal
LCNBV	Ley de la Comisión Nacional Bancaria y de Valores
LFD	Ley Federal de Derechos
LFEA	Ley de Firma Electrónica Avanzada
LFCDO	Ley Federal Contra la Delincuencia Organizada
LFDA	Ley Federal del Derecho de Autor
LFTR	Ley Federal de Telecomunicaciones y Radiodifusión
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTAIP	Ley Federal de Transparencia y Acceso a la Información Pública
LFRPE	Ley Federal de Responsabilidad Patrimonial del Estado
LGPSEDTP	Ley General para Prevenir, Sancionar y Erradicar los delitos en Materia de Trata de Personas.
LGSNSP	Ley General del Sistema Nacional de Seguridad Pública
LGV	Ley General de Víctimas
LIC	Ley de Instituciones de Crédito
LISF	Ley de Instituciones de Seguros y de Fianzas
LOPGR	Ley Orgánica de la Procuraduría General de la República
LSAR	Ley de los Sistemas de Ahorro para el Retiro
LSN	Ley de Seguridad Nacional
LPAB	Ley de Protección al Ahorro Bancario
LPDUSF	Ley de Protección y Defensa al Usuario de Servicios Financieros
PGR	Procuraduría General de la República

CAPÍTULO PRIMERO

MARCO CONCEPTUAL

Para que se logre perpetrar un delito informático a través de una red de datos, primeramente dos equipos de cómputo deben establecer una conexión dedicada de transferencia de paquetes de datos o tramas de información, motivo por el cual es necesario conocer de protocolos de comunicación. Para hacerlo más comprensible, la Organización Internacional de Estandarización ISO desarrolló un modelo constituido por capas de comunicación, para que sin importar quien los fabrique, dos computadoras puedan intercambiar información. En este capítulo describiré cada una de estas capas del modelo OSI, para que de manera deductiva determinemos la importancia del protocolo TCP/IP para la transferencia de información en redes de datos.

1.1. Origen de la Internet

Internet es una colección de redes alrededor del mundo que interactúan a la perfección a través de una arquitectura abierta y sus protocolos asociados. Las tres primeras redes en Internet fueron la Red de Agencias de Proyectos Avanzados de Investigación ARPANET[2](por sus siglas en inglés), la red de paquetes de radio y la red de paquetes por satélite, todos patrocinados por la Agencia de Proyectos de Investigación Avanzados de Defensa DARPA (por sus siglas en inglés), hace varias décadas. Cada una de estas tres redes fue diseñada e implementada individualmente, pero lo más importante, la arquitectura de Internet fue creada para ser independiente del diseño detallado o la implementación de cualquiera de sus redes constituyentes. Como resultado, la tecnología para la creación de redes podría evolucionar y cambiar, de esta

[2] En 1958 se crea ARPA, una agencia de investigación del Departamento de Defensa de los Estados Unidos. Posteriormente pasó a llamarse DARPA. La creación de esta agencia fue la consecuencia tecnológica de la llamada Guerra Fría, y del que surgieron, década después, los fundamentos de ARPANET (red de computadoras Advanced Research Projects Agency Network), red que dio origen a Internet.

manera, la tecnología reciente podría ser integrada con la tecnología anterior simplemente añadiendo nuevas redes.

En 2011, más de un tercio de la población total del mundo tenía acceso a Internet, actualmente más de dos tercios, debido al auge asombroso de conectividad a través de los teléfonos celulares. La llegada de la tecnología 3G (tercera generación) proporcionó la banda ancha de gran velocidad a los teléfonos celulares, 40 veces más rápida que su antecesor, el Servicio General de Paquetes vía Radio GPRS (por sus siglas en inglés), que funcionaba sobre el sistema Acceso Múltiple por División de Tiempo, TDMA (por sus siglas en inglés). Sin embargo, con la aparición del estándar 4G basada completamente en el Protocolo de Internet IP (por sus siglas en inglés), con la capacidad para proveer velocidades de acceso mayores de 100 Mbps en movimiento y 1 Gbps en reposo, lo que permite recibir y enviar datos a velocidades antes imposibles de alcanzar, brindando la posibilidad de reproducir videos en calidad HD y escuchar música directamente desde la nube de datos, entre otros servicios.

En la futura sociedad *hiperconectada,*[3] es difícil imaginar un delito informático, y tal vez cualquier delito, que no implique pruebas electrónicas vinculadas con el protocolo de Internet IP.

1.2. Modelo OSI

El modelo de Interconexión de Sistemas Abiertos OSI (por sus siglas en inglés), es una herramienta de referencia para comprender las comunicaciones de datos entre dos sistemas en red, el cual divide los procesos de comunicación en Siete Capas, figura 1.1.

[3] Greenblatt, Sara, et al, "COMPREHENSIVE STUDY ON CYBERCRIME". *United Nations Office on Drugs and Crime, Draft*, February 2013.

TDMA. El acceso múltiple por división de tiempo (Time Division Multiple Access) es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión.

Cada capa realiza funciones específicas en el proceso de comunicación para soportar las capas superiores, además provee los servicios a las capas inferiores.

Si dividimos en dos partes el modelo, las tres capas más bajas se centran en pasar el tráfico a través de la red a un sistema remoto final, mientras que las cuatro capas superiores entran en juego con el otro extremo en el sistema, es decir, con el usuario o aplicación para completar el proceso de comunicación.

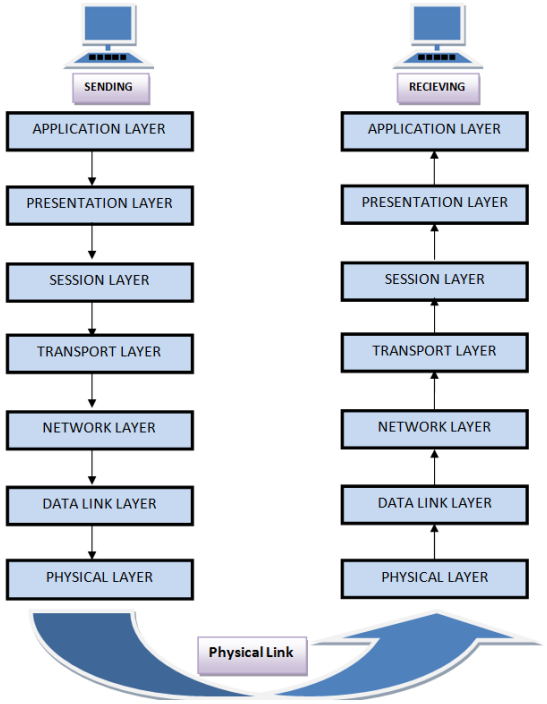

Figura 1.1. Modelo OSI, de Siete Capas.[4]

Un modelo de red ofrece un medio genérico para separar funciones de interconexión de computadoras en múltiples capas; cada una de estas capas se

[4] International Organization for Standardization, https://www.iso.org/ics/35.100/x/. Consulta Junio de 2017

basa a su vez, en las capas por debajo de ella para proporcionar información fuente, hacia las capas superiores. Este modelo de funcionalidad en capas también se denomina "*pila de protocolos*" o "*conjunto de protocolos*".[5]

El modelo de interconexión de sistema abierto es una estructura de siete capas que especifica los requisitos para las comunicaciones entre dos equipos informáticos. La norma ISO-7498-1[6] (Organización Internacional de Estandarización) definió este modelo de siete capas, el cual permite que todos los elementos de red funcionen en conjunto, con independencia de quién creó los protocolos, como fabricante y de qué proveedor los soporta.

Los principales beneficios del modelo OSI son los siguientes: a) Ayuda a los usuarios a comprender el panorama general de las redes, b) Ayuda a los usuarios a entender cómo funcionan los elementos de hardware y software, c) Facilita la resolución de problemas separando las redes en partes manejables, d) Define términos que los profesionales de redes pueden utilizar para comparar relaciones funcionales básicas en diferentes redes, e) Ayuda a los usuarios a entender las nuevas tecnologías a medida que estas se desarrollan y f) Ayuda en la interpretación de las explicaciones de los proveedores sobre la funcionalidad del producto.

CAPA 1: CAPA FÍSICA.

La Capa física del modelo OSI define las especificaciones de conector e interfaz, así como los requisitos del medio (cable, fibra, microondas, etc.). Proporciona especificaciones eléctricas, mecánicas, funcionales y de procedimiento para enviar un flujo de bits en una red de ordenadores.

[5] Simoneau, Paul.The OSI Model: Understanding the Seven Layers of Computer Networks. Global Knowledge, 2006. http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf. Consultado 11 de Junio de 2017, 8:30.
[6] ISO/IEC 7498-1:1994 Preview Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. https://www.iso.org/standard/20269.html. Consultado 11 de Junio de 2017, 11:30

Los componentes de la capa física incluyen: i) Componentes del sistema de cableado, ii) Adaptadores que conectan medios a interfaces físicas, iii) Diseño del conector y asignación de pines, iv) Especificaciones del concentrador, del repetidor y del panel de conexiones, v) Componentes del sistema inalámbrico, vi) SCSI paralelo (interfaz de sistema de computadora), vii) Tarjeta de Interfaz de Red (NIC por sus siglas en inglés), entre otras.

En un entorno de Red de Área Local, LAN (por sus siglas en inglés), el cable UTP (Par trenzado no blindado, por sus siglas en inglés) de Categoría 5e (la "e" de Ethernet), generalmente se utiliza en la capa física para las conexiones de dispositivos individuales; el cableado de fibra óptica se utiliza a menudo para la capa física en un enlace de columna vertebral (*backbone*) o vertical; el IEEE, el EIA/TIA, el ANSI[7] y otros organismos de normas similares desarrollaron estándares para esta capa también.

CAPA 2: CAPA DE ENLACE DE DATOS

La capa 2 del modelo OSI proporciona las siguientes funciones: i) Permite a un dispositivo acceder a la red para enviar y recibir mensajes, ii) Ofrece una dirección física para que los datos de un dispositivo puedan ser enviados a la red, iii) Funciona con el software de red de un dispositivo al enviar y recibir mensajes, y iv) Proporciona capacidad de detección de errores. Los componentes de red comunes que funcionan en la capa 2 incluyen los siguientes dispositivos: a) Tarjetas de interfaz de red, b) Interruptores Ethernet y Token Ring y c) Bridges.

[7] El IEEE, Instituto de Ingeniería Eléctrica y Electrónica, es una de las organizaciones que realiza sus estándares que afectan a una amplia gama de industrias, incluyendo: potencia y energía, biomedicina y salud, tecnología de la información, las telecomunicaciones, el transporte, la nanotecnología, la seguridad de la información. El EIA/TIA, (Alianza de Industrias Electrónicas (EIA) y la Asociación de la Industria de Telecomunicaciones (TIA)) específica en telecomunicaciones, el tipo de cable de par trenzado entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes. El Instituto Nacional Estadounidense de Estándares, más conocido como ANSI (por sus siglas en inglés American National Standards Institute), es una organización que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.

Las NIC tienen una capa 2 o dirección MAC (Control de Acceso al Medio, por sus siglas en inglés). Un switch (conmutador[8]) utiliza esta dirección para filtrar y reenviar el tráfico, ayudando a aliviar la congestión y las colisiones en un segmento de red.

Los bridges y los switches funcionan de una manera similar; sin embargo, el bridging es normalmente un programa de software en una CPU, mientras que los switches utilizan circuitos integrados específicos de la aplicación (ASIC) para realizar la tarea en hardware dedicado, que es mucho más rápido.

CAPA 3: CAPA DE RED

La capa de red del modelo OSI, proporciona un sistema de direccionamiento lógico de extremo a extremo para que un paquete de datos pueda ser encaminado a través de varias redes de capa 2 (v.gr. Ethernet, Token Ring, Frame Relay, etc.). Estas direcciones de la capa de red también pueden denominarse direcciones lógicas.

Inicialmente, los fabricantes de software como Novell, desarrollaron un tratamiento propietario de capa 3; sin embargo, la industria de redes ha evolucionado hasta el punto de que se requiere un sistema de direccionamiento de capa 3 común. Las direcciones de Protocolo de Internet (IP) hacen que las redes sean más fáciles de configurar y conectarse entre sí. Internet utiliza direcciones IP para proporcionar conectividad a millones de redes en todo el mundo.

Para facilitar la administración de la red y controlar el flujo de paquetes, muchas organizaciones separan su dirección de capa de red en partes más pequeñas

[8] Conmutador (switch) es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada ésta. La nueva era del comercio: el comercio electrónico, las TIC al servicio de la gestión empresarial, editorial Idiaspropias, España, 2005. https://books.google.com.mx.
Puente de red (en inglés: bridge) es el dispositivo de interconexión de redes de computadoras que opera en la capa 2 del modelo OSI. Interconecta segmentos de red (o divide una red en segmentos) haciendo la transferencia de datos de una red hacia otra con base en la dirección física MAC de destino de cada paquete.

conocidas como subredes. Los enrutadores utilizan la parte de red o subred del direccionamiento IP para encaminar tráfico entre diferentes redes. Cada enrutador debe configurarse específicamente para las redes o subredes que se conectarán a sus interfaces.

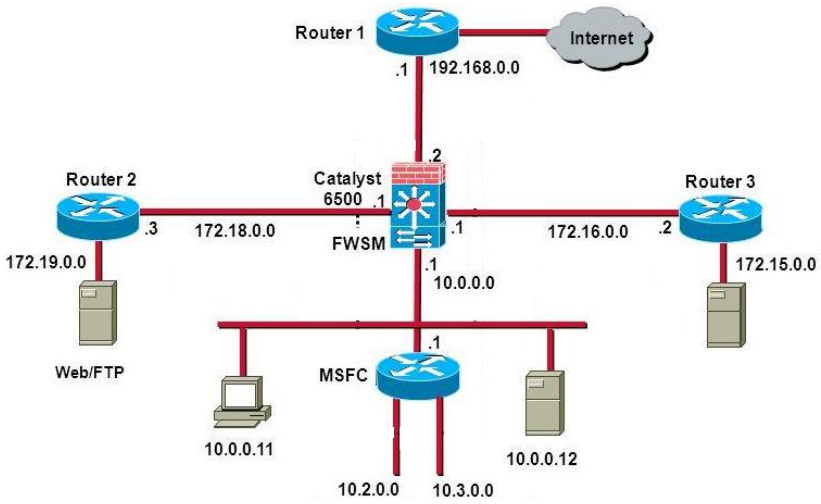

Figura 1.2. Configuración de routing (ruteo) cisco.com[9]

Los routers se comunican entre sí mediante protocolos de enrutamiento, como el Protocolo de información de ruteo RIP (por sus siglas en inglés) o el Primer Camino Más Corto (OSPF por sus siglas en inglés), para conocer otras redes presentes y calcular la mejor manera de llegar a cada red basándose en una variedad de criterios (como el camino con el menor número de routers) ver figura 1.2. Los enrutadores y otros sistemas en red toman estas decisiones de enrutamiento en la capa de red.

Al pasar paquetes entre diferentes redes, puede ser necesario ajustar su tamaño de salida a uno que sea compatible con el protocolo de capa 2 que se está

[9] Redistribución de protocolos de ruteo, Con la colaboración de ingenieros de Cisco. Disponible en https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html, consulta Junio de 2017.

utilizando; la capa de red realiza esto a través de un proceso conocido como fragmentación. La capa de red de un enrutador suele ser responsable de la fragmentación; todo el reensamblado de paquetes fragmentados ocurre en la capa de red del sistema de destino final.

CAPA 4: CAPA DE TRANSPORTE

La capa de transporte del modelo OSI, ofrece comunicación de extremo a extremo entre dispositivos finales a través de una red; dependiendo de la aplicación, la capa de transporte ofrece comunicaciones fiables, orientadas a la conexión o sin conexión, de mejor esfuerzo.

Algunas de las funciones ofrecidas por la capa de transporte incluyen: i) Identificación de la solicitud, ii) Identificación de entidades del lado del cliente, iii) Confirmación de que todo el mensaje llegó intacto, iv) Segmentación de datos para el transporte de la red, v) Control del flujo de datos para evitar sobrecargas de memoria, vi) Establecimiento y mantenimiento de ambos extremos de circuitos virtuales, vii) Detección de errores de transmisión, viii) Realineación de datos segmentados en el orden correcto en el lado receptor y ix) Multiplexar o compartir varias sesiones a través de un solo enlace físico.

Los protocolos de capa de transporte más comunes son TCP (Protocolo de Control de la Transmisión, por sus siglas en inglés) orientado a la conexión y UDP (Protocolo de datagrama de usuario) no orientado a conexión.

CAPA 5: CAPA DE SESIÓN

La capa de sesión, proporciona varios servicios, incluyendo el seguimiento del número de bytes que cada extremo de la sesión ha reconocido recibir desde el otro extremo de la sesión. Esta capa de sesión permite que las aplicaciones que funcionan en dispositivos establezcan, administren y terminen un diálogo a través de una red.

La funcionalidad de la capa de sesión incluye: i) Conexión virtual entre entidades de aplicación, ii) Sincronización del flujo de datos, iii) Creación de unidades de diálogo, iii) Negociaciones de parámetros de conexión, iv) Partición de servicios en grupos funcionales, v) Agradecimientos de los datos recibidos durante una sesión, y vi) Retransmisión de datos si no es recibida por un dispositivo.

CAPA 6: CAPA DE PRESENTACIÓN

La capa de presentación, es responsable de cómo una aplicación formatea los datos que se enviarán a la red; la capa de presentación básicamente permite que una aplicación lea o entienda el mensaje.

Ejemplos de funcionalidad de capa de presentación incluyen: i) Cifrado y desencriptación de un mensaje para seguridad, ii) Compresión y expansión de un mensaje para que viaje eficientemente, iii) Formato de gráficos, iv) Traducción de contenido, y v) Traducción específica del sistema.

CAPA 7: CAPA DE APLICACIÓN

La capa de aplicación, proporciona una interfaz para el usuario final que opera un dispositivo conectado a una red. Esta capa es lo que el usuario ve, en términos de cargar una aplicación; v.g. un navegador Web o un correo electrónico; es decir, esta capa de aplicación son los datos que el usuario ve al utilizar estas aplicaciones.

Ejemplos de funcionalidad de la capa de aplicación incluyen: i) Soporte para transferencias de archivos, ii) Posibilidad de imprimir en una red, iii) Correo electrónico, iv) Mensajería electrónica, v) Navegar por la World Wide Web (www).

> *WWW. Servicio de Internet que permite el acceso a documentos multimedia relacionados entre sí por medio de enlaces. La palabra web, telaraña en inglés, hace referencia a la gran red de enlaces que este servicio crea, ya que cada página web, escrita en HTML, suele hacer referencia a otras páginas web, y así sucesivamente con millones de páginas web repartidas por todo el mundo. Es, en un sentido figurado, una gran telaraña*

que envuelve al mundo (significado más o menos literal de World Wide Web).[10]

1.3. Protocolo TCP/IP

Ahora que ya he tocado el modelo OSI y sus siete capas indispensables para la comunicación entre computadoras, considero que tenemos argumentos para abordar el tema del Protocolo de Control de Transmisión/ Protocolo de Internet TCP/IP (por sus siglas en inglés).

El modelo TCP/IP utiliza cuatro capas para realizar las funciones del modelo OSI de siete capas. La capa de acceso a la red es funcionalmente igual a una combinación de capas OSI físicas y de enlace de datos (1 y 2).

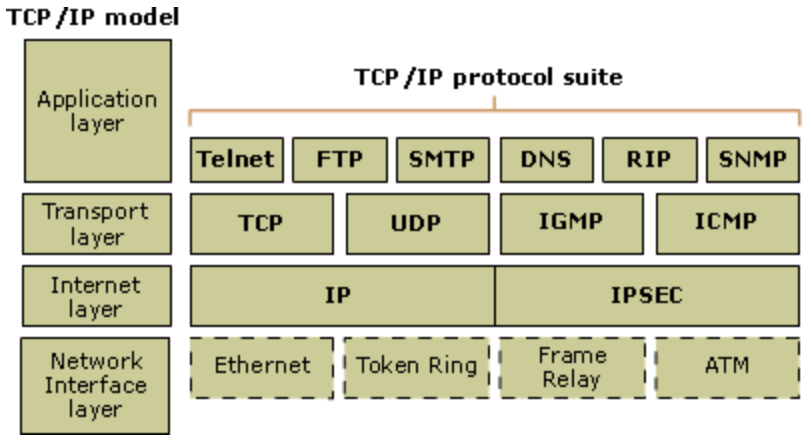

Figura 1.3. Modelo TCP/IP

La capa de Internet realiza las mismas funciones que la capa de red o capa 3 OSI; las cosas se complican un poco más en la capa host-host del modelo TCP/IP. Si el protocolo de host a host es TCP, la funcionalidad de coincidencia se encuentra en las capas de transporte y sesión de OSI (4 y 5). El uso de UDP (*User Datagram Protocol*: en inglés) equivale a las funciones de sólo la capa de transporte del modelo OSI.

[10] Gil García, José Ramón, et al, *Tecnologías de Información y Comunicación en la Administración Pública: Conceptos, Enfoques, Aplicaciones y Resultados*, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, Primera edición, México, 2017, p. 21

La capa de proceso TCP/IP, cuando se utiliza con TCP, proporciona las funciones de las capas de presentación y aplicación del modelo OSI (6 y 7). Cuando el protocolo de capa de transporte TCP/IP es UDP, las funciones de la capa de proceso son equivalentes a las capas 5, 6 y 7 OSI.

Finalmente, algunas de las capas utilizan equipos para soportar las funciones identificadas con anterioridad; la actividad relacionada con el concentrador de cables es Capa Uno; la designación de algunos dispositivos designa la capa funcional como switch de Capa Dos o switch de Capa Tres; las funciones del enrutador se centran en Capa Tres; las estaciones de trabajo y los servidores de usuario suelen identificarse con Capa Siete.

1.4. Protocolo IP

El uso de tecnologías basadas en el Protocolo de Internet, IP es ahora un elemento estratégico en el diseño, desarrollo y uso de las redes de telecomunicaciones. A medida que el uso de redes basadas en IP, incluyendo Internet, continúa creciendo en todo el mundo, se intensifica el diálogo global sobre las funciones y responsabilidades de todos los actores involucrados en la difusión, innovación y uso de estas redes. Internet y las aplicaciones que soporta han adquirido una importancia crucial para el desarrollo económico, social y político de todos los países, en particular los países en desarrollo, ya que la comunidad mundial trata de utilizar el Internet y otras TIC como una manera de ayudar a proporcionar oportunidades digitales para todos.[11]

Todo sistema conectado a un sistema de tipo internet posee un identificador único llamado dirección IP para poder comunicarse, la cual:

Posee una longitud de 32 bits (formando 4 octetos) , v.gr.

10000100.11111000.11001100.00110001 = 132.248.204.49

[11] International Telecommunication Union. A Handbook on Internet Protocol (IP)-Based Networks and Related Topics and Issues. Printed in Switzerland, Geneva, 2005.

Ésta IP posee información del host y de la red a la que pertenece. Teóricamente, la dirección IP de 32 bits permite un máximo de 2^{32} = 4,294,967,296 (Cuatro mil doscientos noventa y cuatro mil millones novecientos sesenta y siete mil doscientos noventa y seis combinaciones) lo que equivale a la misma cantidad de computadoras para ser conectado a Internet en un momento dado. En la práctica, el número total de equipos que se pueden conectar es mucho menor, debido a la forma en que se asignan las direcciones IP. A las organizaciones se les asignan normalmente bloques de direcciones, los cuales no todos son utilizados; este enfoque es similar al método por el cual la compañía telefónica asigna códigos de área a una región. El enfoque ha llevado a un problema con direcciones IP similares a las que enfrenta la compañía telefónica por su limitación y disponibilidad.

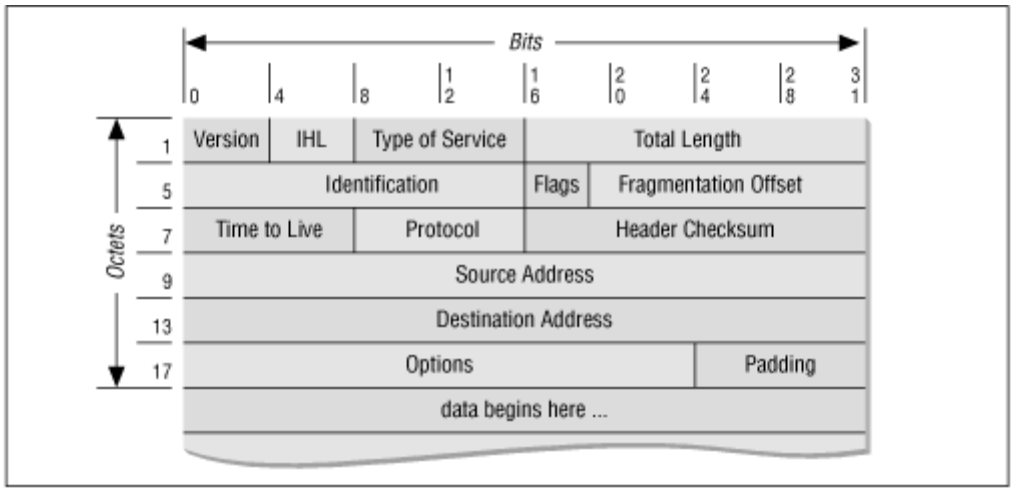

Figura 1.4. Paquete IP[12]

En Internet, los datos se envían en bloques de caracteres llamados datagramas, o más coloquialmente, paquetes; cada paquete tiene un pequeño bloque de bytes llamado el encabezado, que identifica su remitente y destino previsto en cada computadora. El encabezado es seguido por otro, generalmente más grande,

[12] 16. TCP/IP Networks, 16.2 IPv4: The Internet Protocol Version 4, Chapter 16, TCP/IP Networks. https://docstore.mik.ua/orelly/networking/puis/ch16_02.htm, Consulta 17 Junio 2017, 11:00

bloque de caracteres de datos llamados contenidos del paquete; como se visualiza en la figura 1.4; después de que los paquetes llegan a su destino, a menudo se reensamblan en un flujo continuo de datos; este proceso de fragmentación y reensamblaje suele ser invisible para el usuario. Como a menudo hay muchas rutas diferentes de un sistema a otro, cada paquete puede tomar un camino ligeramente diferente de la fuente al destino. Como Internet conmuta paquetes, en lugar de circuitos, se llama una red de conmutación de paquetes. La siguiente tabla describe los campos del paquete IP ilustrados en la Figura 1.4, donde:

Version	Versión: indica la versión de IP que se utiliza actualmente
IHL	Longitud del encabezado IP (IHL): indica la longitud del encabezado del datagrama en palabras de 32 bits.
Type of Service	Tipo de servicio: especifica cómo un protocolo de capa superior desea que un datagrama actual sea manejado, y asigna datagramas varios niveles de importancia.
Total Length	Longitud total: especifica la longitud, en bytes, del paquete IP completo, incluidos los datos y el encabezado.
Identification	Identificación: contiene un entero que identifica el datagrama actual. Este campo se utiliza para ayudar a agrupar fragmentos de datagramas.
Flags	Banderas: Consiste en un campo de 3 bits en el que los dos bits de orden inferior (menos significativo) controlan la fragmentación. El bit de orden baja especifica si el paquete puede ser fragmentado. El bit medio especifica si el paquete es el último fragmento de una serie de paquetes fragmentados. No se utiliza el tercer bit de orden alto.
Fragmentation Offset	Desplazamiento de fragmentos: indica la posición de los datos del fragmento en relación con el comienzo de los datos en el datagrama original, lo que permite que el proceso IP de destino reconstruya correctamente el datagrama original.
Time to live	Tiempo de vida: mantiene un contador que disminuye gradualmente hasta cero, momento en el que se descarta el datagrama. Esto evita que los paquetes se doblen sin fin.
Protocol	Protocolo: indica qué protocolo de capa superior recibe los paquetes entrantes una vez finalizado el procesamiento de IP.
Header Checksum	Checksum de encabezado: ayuda a garantizar la integridad del encabezado IP.
Source Address	Dirección de origen: especifica el nodo emisor.
Destination Address	Dirección de destino: especifica el nodo receptor.
Padding	Relleno: Bits que se agregan para ajustar el paquete a un tamaño específico.

TABLA 1.1. Campos del paquete IP.

1.5. Protocolos de Internet

Este grupo de protocolos, resuelve una serie de tareas relacionadas con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos; los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables. Representan una amplia variedad de servicios, entre las que se incluyen las siguientes:

FTP	Protocolo de transferencia de archivos: mueve archivos entre dispositivos
SNMP	Protocolo simple de administración de red: informa sobre condiciones de red anómalas y establece valores de umbral de red
TELNET	sirve como protocolo de emulación de terminal
X WINDOWS	sirve como un sistema de ventanas y gráficos distribuido utilizado para la comunicación entre terminales X y estaciones de trabajo UNIX
NFS	Sistema de archivos de red, Representación de datos externos (XDR) y RPC (Remote Procedure Call): Trabajar juntos para permitir el acceso transparente a recursos de red remotos
SMTP	Simple Mail Transfer Protocol: Proporciona servicios de correo electrónico
DNS	Sistema de nombres de dominio: traduce los nombres de los nodos de red en direcciones de red.
HTTP	HyperText Transfer Protocol: Protocolo de Transferencia de HiperTexto, es popular porque se utiliza para acceder a las páginas web.
POP	Post Office Protocol: Protocolo de Oficina Postal, para correo electrónico.

TABLA. 1.2. Protocolos de Internet

A manera de resumen del primer capítulo, podemos decir que dos computadoras se interconectan entre sí con el objeto transferir información a través de un modelo de siete capas, donde cada una de ellas tiene asignada una función específica durante la transferencia de información, es importante resaltar que las cuatro primeras capas son fundamentales para lo que nos interesa en este trabajo de tesis, es decir la física, de enlace de datos, de red y transporte, en virtud de que servirán de base para el rastreo de los indicios, vestigios o elementos de prueba de la ciberdelincuencia.

Los paquetes, datagramas o tramas se relacionan con toda la información que se transfiere entre dos equipos informáticos, de tal suerte que su estudio, descripción y análisis será tema del capítulo cinco que comprende la herramienta sugerida para determinar en qué momento una computadora fue intervenida remotamente.

Para evitar cualquier confusión al respecto, me parece oportuno advertir que la tendencia actual hacia una interconectividad móvil, así como un sistema donde todas las cosas se interconecten conocida como IoT (Internet para todo, por sus siglas en inglés), de ninguna manera altera la base fundamental y principios hasta aquí tratados para la interconectividad entre computadoras, como se verá en la siguiente tabla, pues como ya se dijo el modelo de las siete capas es incluyente para cualquier tecnología que se pueda incorporar a las redes ya estructuradas, de lo contrario estaríamos cambiando de técnicas de la comunicación frecuentemente.

Finalmente con la siguiente tabla 1.3 propuesto por ARPA, el cual contiene el resumen de protocolos por nivel de capa OSI, y que ilustra las aplicaciones más recurrentes en materia de intercomunicación de computadoras. Como se ilustra, el protocolo TCP, UDP e IP se ubican en las capas de Transporte y Red respectivamente; independientemente de la aplicación que utilice un hacker, necesariamente deberá enviar la información o comandos a través de estos protocolos.

ARPA Layer	Protocol Implemantation								OSI
	Hipertext Transfer	File Transfer	Electronic Mail	Terminal Emulation	Domain Names	File Transfer	Client Server	Network Manager	7
Process Aplication	HTTP	FTP	SMTP	TELNET	DNS	TFTP	NFS	SNMP	6 / 5
Host to Host	TCP					UDP			4
	Address Resolution			IP			ICMP		3
Internet	Network Interface Cards Ethernet, Tocken Ring, MAN and WAN								2
Network Interface	Transmission Media Twisted Pair, Coax, Fiber Optics, Wireless Media, etc.								1

TABLA 1.3. Protocolos ARPA[13]

[13] A. Miller, Mark, *Internet Technologies Handbook, Optimizing the IP Network*, John Wiley & Sons, Inc, Hoboken, New Jersey, 2004, p. 9

CAPITULO SEGUNDO

MARCO NORMATIVO

El derecho por su carácter regulador de las conductas de las personas en cualquier ámbito de la vida, debe ser parte indispensable de cualquier estudio que involucre una violación a las buenas costumbres o violaciones a derechos de terceros. Lo anterior porque debe ser la base de comparación de cada conducta, toda vez que una sociedad como la mexicana está basada en roles de comportamiento que todos tenemos asignado por el sólo hecho de pertenecer a ella como un sistema de derecho; porque *no existe ninguna otra instancia en la sociedad que pudiera determinar lo que es conforme o discrepante con el derecho*[14]*.*

En sede nacional, hay legislación positiva que regulan el tema relacionado con los sistemas informáticos, desde la CPEUM como catálogo de referencia de los derechos humanos, reconociéndolos e imponiéndoles límites para su ejercicio, hasta la normatividad secundaria que establece las prohibiciones y restricciones de las personas para salvaguardar esos valores axiológicos que la misma sociedad ha determinado como protegidos.

Es así como en este capítulo, sólo se describirá de manera genérica la legislación que define cuándo una conducta es considerada ilícita, y que a la vez sirve como base dentro de la cual las personas deben acotar su actuación dentro de la sociedad. Además, en un contexto internacional el tema de la prevención de la delincuencia es de mayor prioridad para organismos como la ONU que a través de la declaración de Doha, impulsa a los estados parte a entablar una lucha tenaz para combatir la delincuencia. En la próxima tabla sintetizo los instrumentos nacionales como internacionales que de manera directa contienen elementos que enriquecen el estudio de los delitos informáticos, así como su prevención y su combate, y que a la brevedad se desarrollarán en este segundo capítulo.

[14] NIKLAS LUHMANN, El Derecho de la Sociedad, texto electrónico traducción por Juliana Neuenschwander, p.46, disponible en http://lkservicios.com/maestria-2013-1/descargas/517derecho_luhmann.pdf, fecha de consulta 03 de Septiembre de 2017, 11:36.

Sede Constitucional	Constitución Política de los Estados Unidos Mexicanos: Artículos 1, 6, 14, 16, 20 y 21
Leyes secundarias	Código Penal Federal Artículos 211 Bis 1, 2, 3, 4, 5, 6 y 7. Ley Federal de Telecomunicaciones y Radiodifusión. Ley Orgánica Del Poder Judicial De La Federación.
Ámbito Internacional	Declaración de Doha sobre la integración de la prevención del delito y la justicia penal; informe del 13º congreso de las naciones unidas sobre prevención del delito y justicia penal. Doha, Catar 12 a 19 de abril de 2015. Convenio Sobre la Ciberdelincuencia de Budapest, 23.XI.2001; vigente para los Estados miembros del Consejo de Europa.
Jurisprudencia	Registro: 2011880; Interpretación Conforme Registro: 181416; Tipo Penal. Sus Elementos Subjetivos. Registro: 2012525; Garantías del Derecho a la Información.

TABLA 2.1 Marco Jurídico de las telecomunicaciones

2.1. Constitución Política de los Estados Unidos Mexicanos

Constitución publicada en el Diario Oficial de la Federación el 5 de febrero de 1917. Texto Vigente. Última reforma publicada DOF 24-02-2017.

La carta magna del Estado mexicano, en la cual en su primer artículo, establece que todas las autoridades, tienen el deber de implementar políticas públicas encaminadas a promover, respetar, proteger y garantizar los derechos humanos de conformidad con el catálogo estructurado en la misma Constitución y en los tratados internacionales; lo anterior a la luz de los principios de universalidad, interdependencia, indivisibilidad y progresividad. De lo contrario deberán prevenir, investigar, sancionar y reparar las violaciones a los mismos.

En este tenor, su artículo sexto determina que el acceso a las tecnologías de la información y comunicación es un derecho que el Estado debe garantizar considerando las siguientes medidas: i) la información en posesión de cualquier autoridad, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional; ii) la información privada y los datos personales será protegida por la ley; iii) la creación de un organismo autónomo, especializado, para garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales, a la luz de los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad. Así mismo, en este mismo numeral se define que las telecomunicaciones son servicios públicos de interés general, y el Estado las garantizará observando, entre otras cosas, la competencia, la calidad, la pluralidad, cobertura, interconectividad y convergencia.

Así mismo, en el numeral décimo sexto la Constitución determina el derecho de la inviolabilidad de las comunicaciones privadas, incluso eleva a categoría de delito al acto que atente contra la libertad y privacía de las mismas.

Finalmente en el numeral vigésimo primero, la Constitución ordena que el Ministerio Público y las policías son los encargados de la investigación de los delitos, que deberán coordinarse entre sí para cumplir los objetivos de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública; este último contará con las bases de datos criminalísticos y del personal para las instituciones de seguridad pública.

Por otro lado, el Instituto Federal de Telecomunicaciones (IFT).[15] Tiene su fundamento constitucional en el artículo 6º Apartado B, fracción V, y es el organismo del gobierno federal encargado de supervisar el uso y la prestación de servicios adecuados, asociados a la radiodifusión y a las telecomunicaciones en México; garante del derecho de acceso a la información pública y a la protección de datos personales.

[15] IFT Instituto Federal de Telecomunicaciones, http://www.ift.org.mx/sites/default/files/que-es-ift.pdf, consulta Septiembre de 2017.

Según el INEGI la tendencia del uso de las telecomunicaciones y sobre todo el uso de las tecnologías de la información va en aumento. Como puede apreciarse en la siguiente figura 2.1, se refleja una tendencia en aumento del porcentaje anual de los hogares que tienen servicio de banda ancha, así por ejemplo el porcentaje era de 30.70 para el 2014.

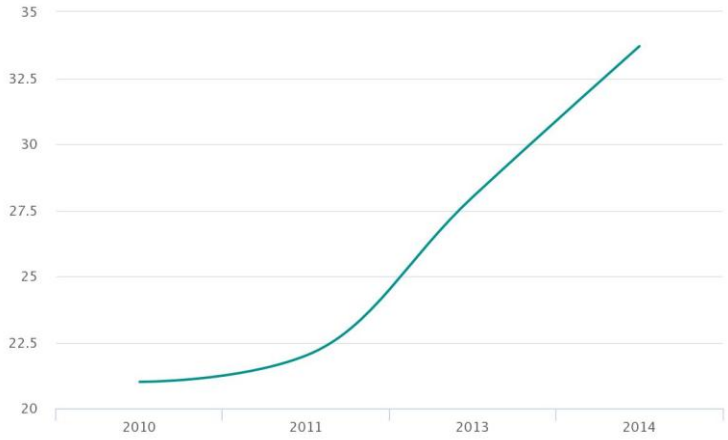

Figura 2.1 Porcentaje anual de hogares con acceso a banda ancha [16]

La gráfica anterior coincide con los datos que proporciona el IFT que en sus reportes trimestrales que publica en su portal web, al arrojar la cifra de 16,213,610 de accesos a tecnologías de la información en el primer trimestre de 2017, es decir 48% de los hogares a nivel nacional y que se ilustran en la figura 2.2.

Además, el Instituto publica que en México existen hasta el mismo periodo la cifra de 77,262,478 de líneas móviles de banda ancha en la República, mostrando un incremento del 181.5% en los últimos 4 años.(ver figura 2.3)

Mientras que las líneas de Telefonía Fija ascendieron a 20,035,720, lo que representa una penetración en los hogares del 60% en números reales, es decir el 9% de incremento en los últimos 4 años. (Figura 2.4)

[16] Fuente: INEGI Módulo sobre Disponibilidad y Uso de Tecnologías de Información en los Hogares 2010-2014. http://www.beta.inegi.org.mx/app/bienestar/#grafica, consulta Septiembre 2017

En resumen, estas imágenes reflejan la clara tendencia en el consumo de servicios de interconectividad en México y lo que en realidad se espera en un futuro con respecto de las conductas ilícitas que han empezado aparecer.

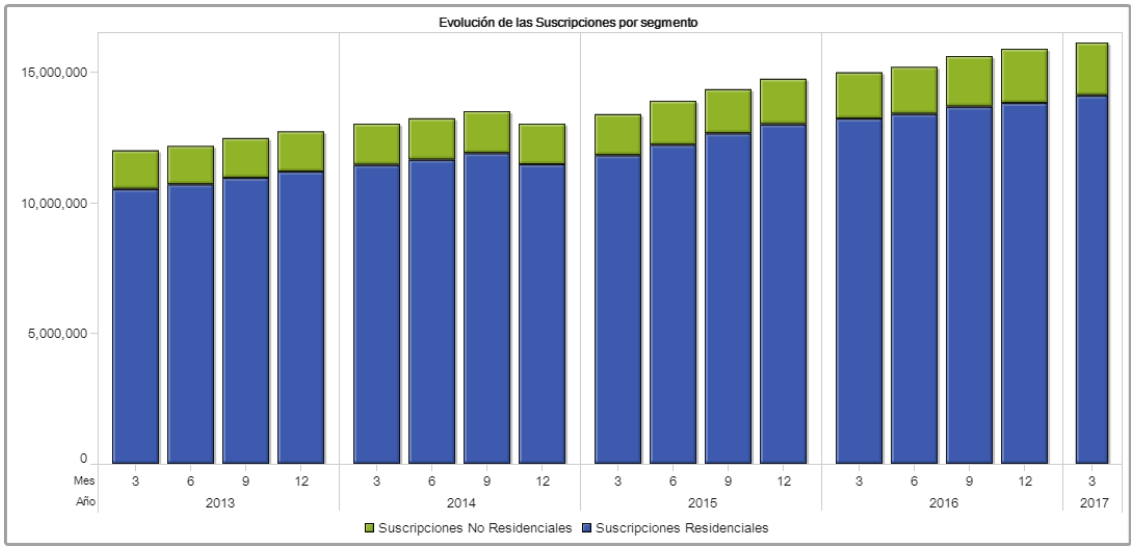

Figura 2.2. Suscripciones Trimestrales de accesos a TIC[17]

Indicador	Datos al 1° Trimestre del 2017	Variación Trimestral del 4° Trimestre del 2016 al 1° Trimestre del 2017	Variación desde la Reforma del 2° Trimestre del 2013 al 1° Trimestre del 2017
Total de líneas de Banda Ancha Móvil (Prepago + Pospago)	77,262,478	2.9%	181.5%
Teledensidad de Banda Ancha Móvil (Prepago + Pospago) por cada 100 habitantes	63	3.3%	173.9%

Figura 2.3. Telecomunicaciones Móviles[18]

[17] IFT Instituto Federal de Telecomunicaciones, https://bit.ift.org.mx/BitWebApp/faces/Reportes.xhtml, consulta Septiembre 2017
[18] íbidem

Indicador	Datos al 1° Trimestre del 2017	Variación desde la Reforma del 2° Trimestre del 2013 al 1° Trimestre del 2017
Total de líneas de Telefonía Fija (Residenciales + No Residenciales)	20,035,720	9.0%
Penetración de líneas de Telefonía Fija (Residenciales + No Residenciales) por cada 100 hogares	60	1.6%
Líneas de Telefonía Fija Residencial	14,974,789	7.4%
Penetración de líneas de Telefonía Fija Residencial por cada 100 hogares	45	0.1%
Porcentaje de líneas Residenciales	74.7%	-1.5%
Líneas de Telefonía Fija No Residencial	5,060,931	14.2%
Penetración de líneas de Telefonía Fija No Residencial por cada 100 unidades económicas	100	14.2%
Porcentaje de líneas No Residenciales	25.3%	4.7%
Líneas de telefonía pública	851,137	
Total de accesos de Banda Ancha Fija (Residenciales + No Residenciales)	16,213,610	33.0%
Penetración nacional de accesos de Banda Ancha Fija (Residenciales + No Residenciales) por cada 100 hogares	49	23.9%
Accesos Residenciales de Banda Ancha Fija	14,141,731	32.0%
Penetración de accesos Residenciales de Banda Ancha Fija por cada 100 hogares	43	23.0%

Figura 2.4. Telecomunicaciones Fijas en México[19]

[19] íbidem

2.2. Código Penal Federal

Nuevo Código Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931. Texto Vigente, Última reforma publicada DOF 26-06-2017

Esta norma sustantiva establece como categoría delictiva el Acceso ilícito a sistemas y equipos de informática en su capítulo segundo del título noveno. Establece las conductas de acción las de ingresar, copiar, modificar, destruir, provocar la pérdida de información contenida en los sistemas o equipos de informática, con o sin autorización de quien pudiera darla, ya sea un particular, el Estado, la instituciones financieras o de seguridad pública; así mismo, establece los tipos de datos cuyo contenido está protegido con la ley.

2.3. Ley Federal de Telecomunicaciones y Radiodifusión.

Ley publicada en el Diario Oficial de la Federación el 14 de julio de 2014; texto vigente, última reforma publicada DOF 27-01-2017.

Esta ley establece una serie de conceptos útiles en materia de telecomunicaciones que deben ser considerados para una mejor comprensión técnica y que a continuación se transcriben los que enlista en su artículo tercero:

> ***Interconexión**: Conexión física o virtual, lógica y funcional entre redes públicas de telecomunicaciones que permite la conducción de tráfico entre dichas redes y/o entre servicios de telecomunicaciones prestados a través de las mismas, de manera que los usuarios de una de las redes públicas de telecomunicaciones puedan conectarse e intercambiar tráfico con los usuarios de otra red pública de telecomunicaciones y viceversa, o bien permite a los usuarios de una red pública de telecomunicaciones la utilización de servicios de telecomunicaciones provistos por o a través de otra red pública de telecomunicaciones.*
>
> ***Internet**: Conjunto descentralizado de redes de telecomunicaciones en todo el mundo, interconectadas entre sí, que proporciona diversos servicios de comunicación y que utiliza protocolos y direccionamiento coordinados internacionalmente para el enrutamiento y procesamiento de los paquetes de datos de cada uno de los servicios. Estos protocolos y direccionamiento garantizan que las redes físicas que en conjunto componen Internet funcionen como una red lógica única.*
>
> ***Red de telecomunicaciones**: Sistema integrado por medios de transmisión, tales como canales o circuitos que utilicen bandas de frecuencias del espectro radioeléctrico, enlaces satelitales, cableados, redes de transmisión eléctrica o cualquier otro medio de transmisión, así como, en su caso, centrales, dispositivos de conmutación o cualquier equipo necesario.*

***Servicios de interconexión**: Los que se prestan entre concesionarios de servicios de telecomunicaciones, para realizar la interconexión entre sus redes e incluyen, entre otros, la conducción de tráfico, su originación y terminación, enlaces de transmisión, señalización, tránsito, puertos de acceso, coubicación, la compartición de infraestructura para interconexión, facturación y cobranza, así como otros servicios auxiliares de la misma y acceso a servicios.*

***Telecomunicaciones**: Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión.*

Esta ley, en su título octavo estipula que los concesionarios de telecomunicaciones y proveedores de servicios de aplicaciones y contenidos están obligados a colaborar con la justicia, es por ello que deberán atender todo mandamiento por escrito, fundado y motivado de la autoridad competente, además de auxiliar a las instancias de seguridad, procuración y administración de justicia, localizando geográfica y en tiempo real los equipos de comunicación móvil de manera efectiva y oportuna; asimismo deberán conservar un registro de las comunicaciones que se realicen de tal suerte que permita identificar con precisión: el nombre, denominación o razón social y domicilio del suscriptor, la clase de comunicación, servicios, la fecha, hora y duración de la comunicación y en general los datos necesarios para rastrear e identificar el origen y destino de las comunicaciones.

Los concesionarios deberán conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales. La información en el registro estará disponible las veinticuatro horas del día y los trescientos sesenta y cinco días del año y cuando sea requerida por las autoridades competentes, la entrega se realizará dentro de las cuarenta y ocho horas siguientes a partir de la notificación de la solicitud. Todo lo anterior de conformidad con la Ley Federal de Protección de Datos Personales

en Posesión de los Particulares, es decir, que la utilización de los datos solo persigue el fin de colaborar con la justicia.

En este orden de ideas, los concesionarios deberán atender los requerimientos para adoptar las medidas necesarias para el bloqueo inmediato de líneas de comunicación, la suspensión inmediata del servicio de telefonía cuando así lo instruya la autoridad competente, o bien cancelen o anulen de manera permanente las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen dentro del perímetro de centros de readaptación social, establecimientos penitenciarios o centros de internamiento para menores.

Finalmente, también obliga a los concesionarios de telecomunicaciones a colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación o de transmisión de datos o imagen. Teniendo presente el derecho de la inviolabilidad de las comunicaciones privadas a menos que la petición sea de autoridad federal.

2.4. Ley Orgánica del Poder Judicial de la Federación.

Ley publicada en el Diario Oficial de la Federación el 26 de mayo de 1995. Última reforma publicada DOF 19-06-2017.

Esta ley decreta la competencia de los jueces federales penales, quienes conocerán de los delitos del orden federal. Estos delitos son: i) los previstos en las leyes federales y en los tratados internacionales; ii) los que se inicien, preparen o cometan en el extranjero y que tengan efectos en el territorio mexicano; cometidos en territorio extranjero por un mexicano contra mexicanos o contra extranjeros; iii) los que involucren a servidores públicos o empleados federales, en ejercicio de sus funciones; iv) los perpetrados en contra del funcionamiento de un servicio público federal o en menoscabo de los bienes afectados a la satisfacción de dicho

servicio; v) que ataquen, dificulten o imposibiliten el ejercicio de alguna atribución o facultad reservada a la Federación.

Además, los jueces federales autorizarán para intervenir cualquier comunicación privada; de la localización geográfica en tiempo real o la entrega de datos conservados de equipos de comunicación asociados a una línea.

2.5. Jurisprudencia de la Suprema Corte de Justicia de la Nación

Este criterio jurisprudencial determina que los elementos normativos como fundamentales que estructuran el tipo penal en un contexto de la teoría del delito cuya observancia es menester en el territorio nacional; asimismo, deben ser valorados verificando su aspecto jurídico, es decir lo previsto en la ley para determinar el contenido y alcance, y además su carácter cultural, para determinar el contenido del elemento que se desea definir.

> *Época: Décima Época; Registro: 2011880; Instancia: Primera Sala; Tipo de Tesis: Aislada; Fuente: Gaceta del Semanario Judicial de la Federación; Libro 31, Junio de 2016, Tomo I; Materia(s): Penal; Tesis: 1a. CLXXIII/2016 (10a.)*
> *Página: 696.*
>
> *INTERPRETACIÓN CONFORME. NO LA CONSTITUYE LA DELIMITACIÓN DEL ALCANCE Y CONTENIDO DE UN ELEMENTO NORMATIVO DEL TIPO PENAL QUE SE REALIZA DESDE UN ÁMBITO DE LEGALIDAD.*
>
> *La teoría del delito proporciona el camino lógico para la incriminación penal, que incluye la conformación de una conducta típica, antijurídica y culpable. En la tipicidad se encuentran los elementos objetivos, entre los que se hallan los descriptivos y los normativos y, por último, los elementos subjetivos específicos o aquellos denominados como requeridos por el tipo penal. Ahora bien,* ***los elementos normativos*** *involucran cierto tipo de valoración para su verificación que puede provenir de: i) un aspecto jurídico, en cuyo caso el juez debe considerar lo previsto en la ley para determinar el contenido y alcance del concepto en análisis; o, ii) un carácter cultural, en donde el juzgador habrá de remitirse a un aspecto social o cultural para determinar el contenido del elemento que se desea definir. Así, el ejercicio de verificación, consistente en la delimitación del alcance y contenido de un elemento normativo del tipo penal, que se realiza desde un ámbito de legalidad, no constituye una interpretación conforme, pues ésta se presenta cuando una norma jurídica es eventualmente contraria a la Constitución Política de los Estados Unidos Mexicanos, por lo que en un ejercicio de interpretación, la autoridad judicial busca armonizarla con lo establecido constitucionalmente o en los tratados internacionales en los que México es parte.*

Este criterio jurisprudencial determina la importancia de los elementos subjetivos del tipo penal obligando a los operadores a su análisis y acreditación, toda vez que la inexistencia de los mencionados elementos, serán las causas de exclusión del delito, como lo establece el numeral 405 del CNPP.

> *Época: Novena Época; Registro: 181416; Instancia: Primera Sala; Tipo de Tesis: Aislada; Fuente: Semanario Judicial de la Federación y su Gaceta; Tomo XIX, Mayo de 2004; Materia(s): Penal; Tesis: 1a. LVI/2004; Página: 517*
>
> *TIPO PENAL. SUS ELEMENTOS SUBJETIVOS, DE CONFORMIDAD CON EL SEGUNDO PÁRRAFO DEL ARTÍCULO 134 DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES, DEBEN SER ANALIZADOS CUANDO SE EJERCE LA ACCIÓN PENAL Y PARA EFECTOS DEL LIBRAMIENTO DE LA ORDEN DE APREHENSIÓN (ADICIÓN PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 18 DE MAYO DE 1999).*
>
> *Si bien el precepto aludido establece que, no obstante lo dispuesto por la fracción II del artículo 15 del Código Penal Federal, el Ministerio Público podrá ejercer la acción penal y que, en su caso, las excluyentes del delito que se actualicen por la falta de **los elementos subjetivos** del tipo serán analizadas por el juzgador después de que se haya dictado el auto de formal prisión o de sujeción a proceso, según corresponda, sin perjuicio del derecho del inculpado de acreditar ante el propio Ministerio Público la inexistencia de los mencionados elementos, ello no significa que se postergue su estudio hasta después de dictarse el auto de procesamiento, sino que establece que serán las causas de exclusión del delito, por falta de dichos elementos, las que serán analizadas por el juzgador después de que se haya dictado el auto citado; además, del proceso legislativo que dio origen a la actual redacción del artículo 134 referido, se concluye que el hecho de que el Ministerio Público al ejercer la acción penal y el Juez al momento de librar la orden de aprehensión, adviertan la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate, a que se refiere el artículo 15, fracción II, del Código Penal Federal, no los releva de la obligación de atender a los datos que acreditan, aun cuando no plenamente, los elementos subjetivos del tipo penal, puesto que de ninguna manera se está facultando a las autoridades que procuran e imparten justicia, para que dejen de analizar dichos elementos en cada una de esas fases procedimentales.*

La siguiente tesis de la SCJN acota el derecho a la información, declarando la facultad y la obligación del Estado mexicano para garantizar su acceso, búsqueda, difusión, restricción de la información contenida en archivos, registros, datos y documentos públicos.

Época: Décima Época; Registro: 2012525; Instancia: Segunda Sala; Tipo de Tesis: Aislada; Fuente: Gaceta del Semanario Judicial de la Federación; Libro 34, Septiembre de 2016, Tomo I; Materia(s): Constitucional; Tesis: 2a. LXXXV/2016 (10a.); Página: 839

DERECHO A LA INFORMACIÓN. GARANTÍAS DEL.

De conformidad con el texto del artículo 6o. constitucional, el derecho a la información comprende las siguientes garantías: 1) el derecho de informar (difundir), 2) el derecho de acceso a la información (buscar) y, 3) el derecho a ser informado (recibir). Por un lado, el derecho de informar consiste en la posibilidad de que cualquier persona pueda exteriorizar o difundir, a través de cualquier medio, la información, datos, registros o documentos que posea. En ese sentido, exige que el Estado no restrinja ni limite directa o indirectamente el flujo de la información (obligaciones negativas), y por otro lado, requiere que el Estado fomente las condiciones que propicien un discurso democrático (obligaciones positivas). Por otro lado, el derecho de acceso a la información garantiza que todas las personas puedan solicitar información al Estado respecto de los archivos, registros, datos y documentos públicos, siempre que sea solicitada por escrito, de manera pacífica y respetuosa. Al respecto, exige que el Estado no obstaculice ni impida su búsqueda (obligaciones negativas), y por otro lado, requiere que establezca los medios e instrumentos idóneos a través de los cuales las personas puedan solicitar dicha información (obligaciones positivas). Finalmente, el derecho a ser informado garantiza que todos los miembros de la sociedad reciban libremente información plural y oportuna que les permita ejercer plenamente sus derechos, quedando obligado el Estado a no restringir o limitar la recepción de cualquier información (obligaciones negativas) y por otro lado, también exige que el Estado informe a las personas sobre aquellas cuestiones que puedan incidir en su vida o en el ejercicio de sus derechos, sin que sea necesaria alguna solicitud o requerimiento por parte de los particulares (obligaciones positivas).

2.6 Declaración de Doha

La Declaración de Doha fue aprobada por aclamación en el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal que se celebró en Doha, capital de Qatar en abril de 2015. Donde fortalece el compromiso común de defender el estado de derecho y prevenir y combatirla delincuencia en todas sus formas y manifestaciones. Por ende en la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco contiene el más amplio programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y promover el Estado de Derecho a nivel Nacional e Internacional. Con la participación pública se pretende defender el estado de derecho y prevenir y combatir la delincuencia y garantizar que nuestros sistemas

de justicia penal sean eficaces, imparciales, humanos y responsables, facilitar el acceso a la justicia para todos, crear instituciones eficaces, responsables, imparciales e inclusivas a todos los niveles.

2.7 Convenio Sobre la Ciberdelincuencia de Budapest, 23.XI.2001

Pareciera que, después de casi 16 años de su firma de este convenio y 13 de su entrada en vigor, perdiera vigencia; sin embargo, su contenido prevalece y se fortalece día con día, debido al desarrollo impresionante que ha traído la tecnología, sobre todo en el ámbito de las telecomunicaciones y tecnologías de la información. Signado por los Estados miembros del Consejo de Europa, este Convenio, es considerando clave de una unión más estrecha entre sus miembros para intensificar la política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, esto mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

A través de sus 48 artículos, este convenio establece la directriz principal para los Estados miembros contra la ciberdelincuencia, manejando los conceptos informáticos más relevantes, así como los delitos informáticos clasificados en cuatro grupos principalmente: i) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, ii) Delitos informáticos, iii) Delitos relacionados con el contenido y iv) Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Además, sugiere la tipificación de entre otros delitos: El acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos, falsificación informática, fraude informático y delitos relacionados con la pornografía infantil.

> *La Convención ha ido perfeccionando sus preceptos, por ejemplo, con el protocolo adicional relativo a la incriminación de actos de racismo y xenofobia a través de sistemas informáticos del 28 de enero de 2003 en Estrasburgo, así como la de Lanzarote del 25 de*

Octubre de 2007 en materia de explotación y abuso sexual infantil.[20]

En síntesis podemos afirmar que el estrecho camino que tenemos las personas para conducirnos a través de los sistemas informáticos está delimitado por un marco normativo que estructuralmente establece los derechos a la información pública, a la libertad de expresión, así como el acceso a las tecnologías de información; además, define las fronteras de la buena conducta que todo ciudadano está obligado a observar.

Ahora que se ha definido globalmente el quinto espacio (ciber espacio) surge también la necesidad imperiosa de regular no sólo su aspecto técnico y tecnológico, sino también su aspecto legal, toda vez que las personas interactúan a través de dispositivos electrónicos de comunicación acarreando consecuencias como: violaciones de propiedad, personal, incluso de la vida.

Sobre la teoría del Internet de las cosas, donde ya no habrá objeto alguno con características de procesamiento electrónico que esté aislado, sino que estará interconectado a través de la red de redes como el internet, y como ya se vio en el primer capítulo de esta tesis, una vez que los dispositivos de comunicación se interconectan, cualquier persona que se localice en cualquier parte de este pequeño mundo podrá irremediablemente ingresar a ellos y conducirse de una forma dolosa afectando su funcionamiento; así, v.gr. un hacker[21] [22] podría tomar el

[20] Téllez Carbajal, Evelyn, Derecho y TIC. Vertientes actuales, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, núm. 751, México 2016, p. 304.

[21] "*Es cualquier persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador congénito que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información*" Palomá Parra, Luis Orlando, *Delitos informáticos en el ciberespacio*, Ediciones Jurídicas Andrés Morales, Colombia, 2012, p.63

[22] Los primeros hackers se apasionaban por la tecnología y sentían una necesidad imperiosa de saber cómo funcionaba todo, y la palabra hacker no tenía la connotación negativa como lo tienen ahora. "*The early hackers had a love of technology and a compelling need to know how it all worked, and their goal was to push programs beyond what they were designed to do. The word hacker did not have the negative connotation as it has today"* Akhgar, Babak, et al, *Ciber Crime and Ciber Terrorism Investigator's HandBook*, Copyright 2014, Elsevier Inc. USA, p.158

control de un automóvil que se conduce de forma autónoma, provocando cualquier tipo de percance; o bien un marcapasos que esté conectado a internet podría verse alterado por alguien que quisiera provocar la pérdida de la vida a un paciente; o peor aún qué pasaría si el control de una aeronave comercial es *hackeada* provocando una catástrofe mortal.

Por todo lo anterior, es fundamental seguir con el estudio y mejora de la legislación mexicana para empatarla a las necesidades vigentes, porque desde mi punto de vista, el Derecho está años de distancia con el desarrollo de la tecnología y si aún no concientizamos ésta necesidad, entonces no hemos comprendido que el derecho es un ente viviente que cambia constantemente.

CAPITULO TERCERO

MARCO TEÓRICO

3.1. Delitos Informáticos

Los delitos en el campo de las computadoras son un campo bastante nuevo porque la sustancia misma de la legislación penal ha aparecido sólo en los últimos años, debido a los asombrosos avances que se han producido en la teoría de los sistemas, en la cibernética, tecnología computacional, telecomunicaciones y sobre todo en internet.

El término cibercrimen se puede traducir como delincuencia informática como lo han llamado en España, se trata de un término que implica delitos cometidos a través del internet, que ha sustituido al que se venía utilizando de delincuencia informática, pero hoy éste ya no tiene mucho sentido.

> *Es importante mencionar que lo que se sanciona es la conducta de la persona, las redes, internet y las computadoras sólo se han vuelto un medio para la comisión de estos delitos; sin embargo, estos medios han hecho que también sean diferentes las interacciones entre la víctima y el delincuente y por ende, se requiere hacer varios ajustes tanto en la argumentación penal como en la legislación.*[23]

El término ciberdelincuencia se encuentra aún en la mesa de debate en cuanto a la legislación de muchos países del mundo, incluyendo a México; sin embargo, a partir del atentado del 11 de Septiembre de 2001 contra las Torres Gemelas en la ciudad de Nueva York, Estados Unidos, el cual fue planeado y ejecutado a través del uso y aprovechamiento de las tecnología de la información y comunicaciones, así como de la amenaza global del terrorismo digital, dirigido al ataque de sistemas financieros, sistemas de defensa, bases de datos, difusión de virus, entre otros factores, trajo como consecuencia que en la actualidad se trabaje de manera

[23] Huerta Estefan, Janet, "*Frente a la Cibercriminalidad más que buenas leyes se requiere prevención: Javier Fernández Teruelo*", *Revista Foro Jurídico*, México, Núm. 165, junio 2017, p.9

seria y globalizada en la generación y aplicación de leyes enfocadas a castigar conductas delictivas cometidas mediante la utilización de equipos de cómputo y sistemas de comunicación, ya sea como fin o como medio.[24]

La doctrina ha denominado a este grupo de comportamientos, de manera genérica, delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática.[25] Pero todos tienen un factor en común, porque se trata de delitos del fuero común, que tienen como medio comisivo en su mayoría el internet.

Robin Bryant, refiere que "*en el discurso actual, sobre la investigación del delito y dentro de la comunidad académica, se utilizan una serie de términos relacionados con el advenimiento de nuevas formas de criminalidad asociadas con el crecimiento de las tecnologías digitales"*.[26] Términos entre otros como: crimen de nueva tecnología, crimen en línea, crimen informático, crimen de red, crimen de internet, crimen virtual, robo de propiedad electrónica crimen electrónico, crimen post moderno, cibercrimen ciber-pornografía, ciber-terrorismo, ciber-acoso, etcétera, como puede apreciarse en la figura 3.1., la cual contiene los términos en su idioma original.

Se estima que alrededor del mundo existen más de 13 tipos de delitos informáticos[27], dentro de los cuales destacan: el acceso ilegal a una red, intercepción ilegal de datos informáticos, interferencias ilegales con un sistema informático o datos informáticos, herramientas de uso indebido en la computadora, fraude relacionado con la informática, falsificación relacionada con la informática,

[24] Sergio García Ramírez, Olga Islas de González Mariscal. *Derecho Penal Y Criminalística*, XII Jornadas sobre Justicia Penal. Instituto de Investigaciones Jurídicas, Serie de Estudios Jurídicos, Núm. 2018, UNAM, México 2012. https://archivos.juridicas.unam.mx/www/bjv/libros/7/3169/15.pdf consulta: 23 Junio 2017.
[25] Santiago Acurio Del Pino, Santiago. *Delitos Informáticos: Generalidades*. Pontificia Universidad Católica del Ecuador. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf. Consulta 24 junio 2017, 11:50 hrs.
[26] Bryant, Robin, *Investigating Digital Crime*, Canterbury Christ Church University, UK. John Wiley & sons Ltd, p.17, "*In popular discourse, in crime investigation and within the academic community, a number of terms are used relating to the advent of new forms of criminality associated with the growth of digital technologies*".
[27] Greenblatt, Sara, op. cit. nota 3, p.78

delitos de robo de identidad, delitos de copyright o marcas registradas, correo no deseado o spam, racismo y xenofobia, pornografía infantil, ciberterrorismo y grooming infantil.

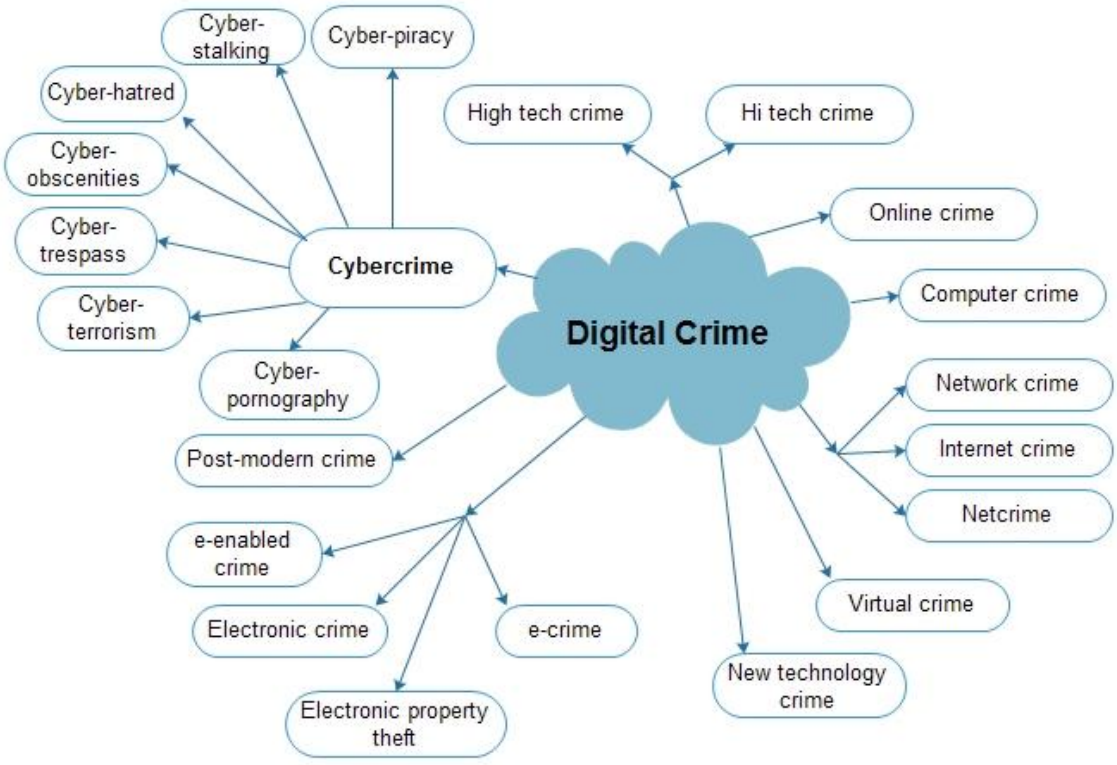

Figura 3.1. Crimen digital y sus vertientes[28]

Así mismo, se le llama evidencia electrónica a todo el material que existe en forma electrónica, o digital, el cual puede ser almacenado o transmitido a través de redes de telecomunicaciones; es decir puede existir en forma de archivos informáticos, transmisiones, registros, metadatos o datos de red.

[28] Bryant Robin, op. cit. nota 26, p. 17

ATAQUES INFORMÁTICOS

Se identifican distintos tipos de ataques informáticos, Gómez Vieites los diferencia en Ataques activos y ataques pasivos; los primeros producen cambios en la información y en la situación de los recursos del sistema, y los segundos sólo se limitan a registrar el uso de los recursos accediendo a la información guardada o transmitida por el sistema, como él mismo los ilustra en la figura 3.2.

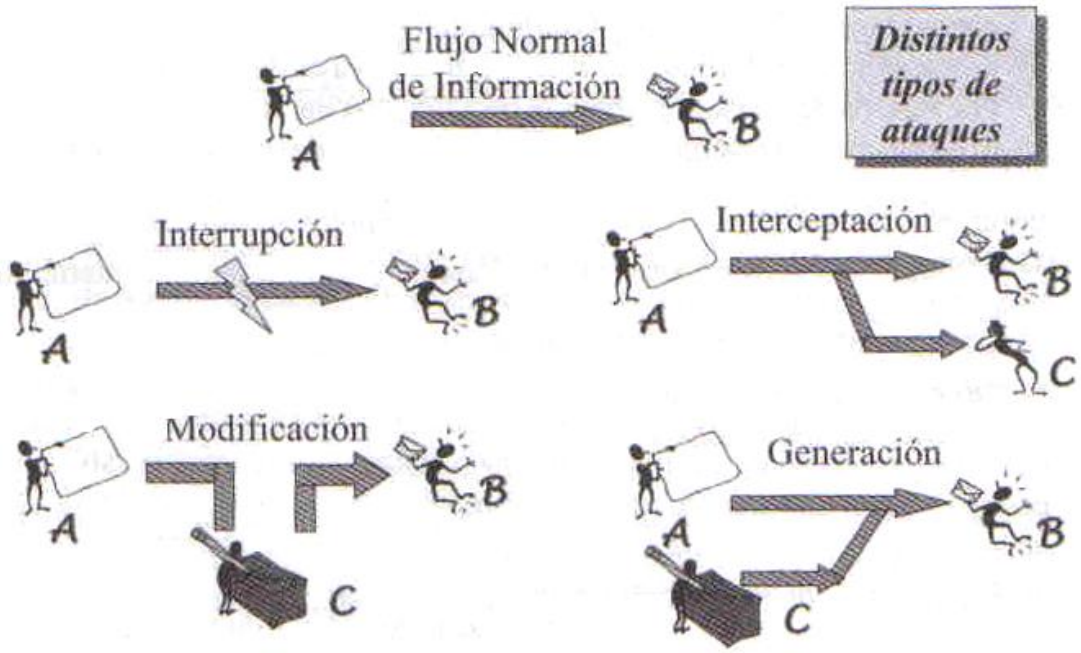

Figura 3.2. Tipos de ataques informáticos[29]

Los ataques se materializan debido a las vulnerabilidades de seguridad, las cuales se derivan por cualquier tipo de defecto en software o hardware. Así, después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla. Un ataque es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida. El acto de

[29] Gómez Vieites, Álvaro, *Enciclopedia de la seguridad informática*, 2a Edición Actualizada, Alfaomega, 2011, p. 204

aprovecharse de una vulnerabilidad se conoce como ataque. El objetivo del ataque es acceder a un sistema, los datos que aloja o recursos específicos sin importar que se hayan configurado los permisos de un archivo, el sistema operativo no puede evitar que alguien lo vulnere y lea los datos directamente del disco.

Existen diferentes maneras en que los atacantes pueden infiltrarse en un sistema dentro de las cuales se encuentra el uso de malware como:

Spyware: Este malware está diseñado para rastrear y espiar al usuario. A menudo modifica las configuraciones de seguridad.	**Adware**: El software de publicidad está diseñado para brindar anuncios automáticamente, pero también es común que el adware incluya spyware.	**Bot**: De robot, un bot es diseñado para realizar acciones automáticamente, en línea.[30]
Ransomware: Diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago.	**Scareware**: Diseñado para persuadir al usuario de realizar acciones específicas en función del temor.	**Rootkit**: Diseñado para modificar el sistema operativo a fin de crear una puerta trasera para acceder a la computadora de forma remota
Virus: Es un código ejecutable malintencionado que se adjunta a otros archivos ejecutables, generalmente programas legítimos.	**Troyano**: Es malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada.	**Gusanos**: Son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes.

Tabla 3.1 tipos comunes de malware

A continuación, abordaré brevemente cada uno de estos delitos describiendo en qué consisten, qué tipo de malware emplean, cual es la legislación en sede

[30] Amoroso, Edward G., Cyber Attacks, *Protecting national infrastructure*, Elseiver, USA, 2011, p.8. Una amenaza Botnet implica el control remoto de una colección de máquinas comprometidas del usuario final, generalmente las PC conectadas de banda ancha.

internacional, así como nacional que la tipifican para que de esa forma, esta conducta pueda ser considerada ilícita y antijurídica.

3.1.1. El acceso ilegal a una red

Acceder a un sistema informático sin autorización adecuada ha existido desde los primeros días del desarrollo de las tecnologías de la información. El acceso ilegal amenaza intereses como la integridad de los sistemas informáticos. El bien jurídico se infringe no sólo cuando una persona sin autorización altera o roba datos en un sistema informático ajeno, también cuando el autor simplemente revisa en el sistema informático, es decir, con el simple hecho de accesar, infringe la confidencialidad de los datos, y pueden requerirse acciones considerables por parte de la víctima para comprobar la integridad o el estado del sistema; en suma, el simple acceso a un sistema informático ya es considerado ilegal en la mayoría de los países europeos, porque no requiere que el infractor acceda a los archivos del sistema u otros datos almacenados.

> "*La punibilidad del acceso ilegal, por lo tanto, representa un elemento disuasorio importante para muchos otros actos posteriores contra la confidencialidad, integridad y disponibilidad de sistemas o datos informáticos y otros delitos informáticos, como el robo de identidad y el fraude o la falsificación informática*".[31]

Estas condiciones permiten a los Estados adoptar una legislación más restrictiva sobre el acceso ilegal; de hecho, el estudio sobre ciberdelincuencia de la Oficina de Las Naciones Unidas sobre Drogas y Crímenes con sede en Viena revela que el consenso no es universal en cuanto a la conveniencia de penalizar el mero acceso ilegal a sistemas no protegidos. Por otro lado, algunas condiciones proporcionadas por los enfoques internacionales, especialmente aquéllos que incluyen requisitos para actos adicionales, pueden plantear dificultades para

[31] Greenblatt, Sara, op. cit. nota 3, p.82.

distinguir el acceso ilegal y otros delitos como la interferencia de datos o el espionaje de datos.

En este orden de ideas, todos los instrumentos multilaterales requieren que el delito de acceso ilegal sea cometido intencionalmente; sin embargo, la definición de lo que constituye la *intención* generalmente se deja al criterio de cada país que implemente este delito; incluso, el Informe Explicativo de la Convención sobre Cibercriminalidad del Consejo de Europa establece explícitamente que el significado exacto de *intencionalmente* debería ser dejado a la interpretación local. A este respecto, en México tenemos que el aspecto subjetivo genérico de la conducta tiene dos vertientes el dolo y la culpa y en consecuencia difiere entre muchos ordenamientos jurídicos internacionales que dependen del derecho penal especial y general.

> *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…*

La legislación mexicana en el Código Penal Federal se tipifica este delito informático como *"Acceso ilícito a sistemas y equipos de informática*". Así por ejemplo el tipo penal contenido en el artículo 211 bis 1, considera como sujeto activo a cualquier persona sin distinción, el elemento subjetivo genérico dolo, porque quien ingresa a un sistema informático quiere y acepta el resultado típico de la pérdida de información; como elementos objetivos contempla las conductas que se concretan en la forma de acción, entendida ésta como un movimiento corporal voluntario, consistente en un actuar positivo, prohibido por la norma penal, y las cuales van más allá del simple acceso porque refiere que el sujeto debe modificar, destruir o provocar pérdida de información, consecuentemente, esto vuelve al delito complejo y difícil de actualizar porque además exige una cualidad específica en el objeto material, el relacionado con los mecanismos de seguridad informáticos, los cuales son aquellos dispositivos constituidos de software y hardware diseñado para detectar, prevenir o recuperarse de un ataque

de seguridad, v.gr., antivirus, firewalls, escudos, etcétera; demás contiene el elemento normativo sin *autorización*, el cual en su segunda acepción del diccionario de la lengua española se lee "*Acto de una autoridad por el cual se permite a alguien una actuación en otro caso prohibida*"; que en el contexto que nos ocupa, se entiende que la autorización deviene del propietario del sistema o equipo informático.

Finalmente el Convenio sobre la Cibercriminalidad del Consejo de Europa ha establecido la siguiente directriz sobre el *Acceso ilícito*:

> *Artículo 2 - Acceso ilícito*
>
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.*

Sobre éste aspecto, la convención de Budapest es clara al especificar que los Estados parte de la convención tienen la libertad de tipificar el delito de "*El acceso ilegal a una red",* conforme a su legislación interna estableciendo el grado de punibilidad de conformidad con los usos y costumbres de cada país.

3.1.2. Intercepción ilegal de datos informáticos

La penalización de la intercepción ilegal se relaciona con la protección de la integridad y confidencialidad de los datos informáticos, ya sea que estos datos residan en un sistema o que sean datos transmitidos. Una preocupación fundamental detrás de la prohibición de la interceptación de datos informáticos en la transmisión, es la violación de la confidencialidad en las comunicaciones privadas.

En muchos países existen infracciones específicas relativas a la intercepción de datos informáticos, incluidas las prohibiciones de intercepción de las

comunicaciones en general; así, la intercepción de datos informáticos involucra dos aspectos fundamentales; por una parte la integridad de los datos, y por la otra, la protección de la privacidad.

En cuanto al concepto de *transmisión*, significa que los datos pueden considerarse en transmisión cuando no han alcanzado el destino final, ya sea el sistema origen o el destinatario. Se podría considerar que la transmisión de datos finaliza cuando se alcanza el sistema informático de destino. También, los datos pueden ser considerados en *transmisión*, cuando se almacenan en el sistema hasta que el destinatario objetivo tenga acceso a ellos. La distinción es importante con respecto al almacenamiento temporal de datos que se produce cuando se transmiten datos informáticos con el uso de protocolos operados en una base de almacenamiento y envío.

El delito de interceptación ilegal de transmisión de datos por ordenador se considera como una delincuencia complementaria en relación con el acceso, sin derecho, a un sistema informático. En realidad, en muchos casos, ambos delitos pueden existir en una relación consecuente.

En la legislación mexicana, la propia CPEUM en su última reforma publicada DOF 24-02-2017, en su última reforma publicada DOF 24-02-2017, en su numeral 16 párrafo décimo segundo, establece que las comunicaciones privadas son inviolables, además considera la excepción.

> *Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*

Aunque este texto está relacionado con las llamadas telefónicas, con una interpretación del término "*comunicaciones"* involucra cualquier comunicación

incluso las que no son electrónicas, de esta manera está implícita la comunicación entre sistemas informáticos.

En este orden de ideas, muchos instrumentos legales cibernéticos multilaterales en el mundo[32], definen la interceptación ilegal como transmisión "no pública" de datos informáticos, es decir limitan así el objeto a transmisiones "privadas"; esta limitación se refiere a la naturaleza pretendida de la transmisión. V.gr., una comunicación que tiene carácter privado pero se envía a través de la red Wi-Fi pública puede protegerse para fines de interceptación ilegal, aunque la transmisión pase a través de una red pública.

Además de las transmisiones no públicas, también cubren la interceptación de las "transmisiones electromagnéticas", un término también utilizado para ampliar el alcance del delito. En la práctica, sin embargo, debido a la interpretación amplia de "no público", es probable que esto no amplíe significativamente el alcance de la lesión al bien jurídico tutelado.

Finalmente el Consejo de Europa en la Convención de Ciberdelincuencia en su artículo 5 ofrece a las partes la posibilidad de limitar el delito de interceptación ilegal a los casos cometidos dolosamente:

> *Artículo 5 - Interferencia en el sistema*
>
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de datos, borrado, deterioro, alteración o supresión de datos informáticos.*

3.1.3. Interferencias ilegales con un sistema informático o datos informáticos

Los datos informáticos son vitales para los usuarios privados, las empresas y las administraciones, todos los cuales dependen de la integridad y la disponibilidad de los datos. La falta de acceso a los datos puede resultar en un daño financiero

[32] Ibídem p.86.

considerable. La interferencia con datos o sistemas informáticos pone en peligro su integridad y su disponibilidad, así como el correcto funcionamiento de los programas y los sistemas informáticos. Debido a la naturaleza no tangible de los datos informáticos, muchos sistemas jurídicos en el mundo pueden no ser capaces de ampliar las disposiciones tradicionales del derecho penal relativas a la destrucción de la propiedad física a la interferencia de datos informáticos.

Los infractores pueden violar la integridad de los datos e interferir con ellos eliminando, suprimiendo o alterando los datos de la computadora. Un ejemplo común de la supresión de datos es el virus informático. Desde que se desarrolló por primera vez la tecnología informática, los virus informáticos han amenazado a los usuarios que no instalaron la protección adecuada. Desde entonces, el número de virus informáticos ha aumentado significativamente y mejorado sustancialmente las técnicas y funciones de los virus. Anteriormente, los virus informáticos se distribuían a través de dispositivos de almacenamiento, como los disquetes, mientras que hoy en día la mayoría de los virus se distribuyen a través de Internet como archivos adjuntos a correos electrónicos o archivos que los usuarios descargan.

> *La suplantación de datos consiste en agregar, modificar o eliminar datos presentes en un paquete que se mueve en una red.*
>
> *Se trata de un archivo que da una extensión diferente a la real, engañando así al usuario. Esta técnica también es utilizada por virus, ocultos detrás de extensiones de archivo "tranquilizadoras" como .jpeg o .zip, que realmente contienen archivos ejecutables (.exe).*
>
> *El modus operandi script-kiddies es diferente. En primer lugar, exploran Internet buscando sistemas con vulnerabilidades conocidas para las que han escrito o copiado secuencias de comandos que les permiten tomarlo y explotarlo con un acceso root. Entonces comienzan Web desfigurar; reemplazan la página principal del sitio Web de destino con una nueva página que contiene un mensaje que informa al administrador del sistema de que el servidor es vulnerable a ataques. Normalmente no destruyen los datos presentes en los sistemas violados; en realidad, casi siempre guardan la página web original y explican a SysAdmin dónde encontrarla.*[33]

[33] Chiesa, Raoul, et al, *Profiling Hackers, The Science of Criminal Profiling as Applied to the World of Hacking,* Taylor & Francis Group, LLC, 2009, p.136

Las mismas preocupaciones sobre los ataques contra datos informáticos se aplican para ataques contra sistemas informáticos. Los ataques pueden ser llevados a cabo por físicamente al sistema informático, los cuales pueden destruir el hardware; estos ataques no plantean problemas importantes, ya que son similares a los casos clásicos de daño o destrucción de la propiedad. Sin embargo, para los negocios de comercio electrónico, los daños financieros causados por los ataques al sistema informático son mucho mayores que el simple costo del hardware de la computadora; ejemplos de ataques remotos contra sistemas informáticos son los que incluyen virus o gusanos de computadora y ataques de denegación de servicio DoS.

Para la mayoría de las legislaciones europeas, la interferencia de los datos y la interferencia del sistema figuraban en disposiciones separadas. Sin embargo, los delitos no están claramente separados o la injerencia de datos sólo se penaliza cuando tiene un efecto sobre el funcionamiento de un sistema informático.

En algunos países esto todavía puede estar cubierto por las leyes penales generales. Por ejemplo, un país de las Américas hace uso de una disposición general sobre la destrucción o la producción de *bienes* defectuosos, en la que la definición de *bienes* incluye datos informáticos. Como es el caso de México donde el mismo artículo 211 BIS 1, revisado en el tipo de *Acceso Ilegal*, el cual abarca también este tipo penal de *Interferencias ilegales con un sistema informático o datos informáticos* porque considera como verbos rectores la modificación, la destrucción y la pérdida de información contenida en sistemas o equipos de informática, asimismo el 211 BIS 2, que define al sujeto pasivo que en este caso es el gobierno quien aparece como propietario de los sistemas y datos informáticos. Para los 211 BIS 3 y 211 BIS 4 los cuales a diferencia de los dos anteriores el sujeto activo ejecutor de la conducta es una persona autorizada para acceder al sistema o datos informáticos, finalmente el Código Penal Federal también contiene el numeral 211 BIS 5 donde se agrega una calidad específica al sujeto pasivo o víctima u ofendido del delito, quien en este caso son las instituciones financieras.

De esta manera los instrumentos internacionales contemplan la penalización de diferentes actos que constituyen una interferencia de datos, incluyendo no sólo el daño a los datos, sino también la supresión, el deterioro, la alteración de datos en un sentido extenso. No obstante sólo un grupo reducido de países penalizan la *transmisión* de datos con arreglo a disposiciones sobre interferencia de datos. Podría esperarse que la transmisión de datos se tipificara como delito en países en los que los datos y las interferencias de los sistemas están cubiertos por una disposición, ya que la transmisión de datos podría afectar al sistema.

De la misma forma que los datos informáticos, los sistemas informáticos pueden ser dañados de diversas maneras, por ejemplo en la transmisión, alteración o supresión de datos, por interferencia electromagnética o incluso cortando el suministro eléctrico. Como es el caso de la Ley Modelo del Commonwealth[34] y en los Textos Legislativos Modelo ITU/CARICOM/CTU[35], que incluyen no sólo la manipulación de datos, sino también cortar el suministro de electricidad a un sistema informático, causando interferencias electromagnéticas y corrupción a un sistema informático por cualquier medio.

3.1.4. Herramientas de uso indebido en la computadora

El software y otras herramientas utilizadas para cometer crímenes en el entorno digital, así como las contraseñas de las víctimas y los códigos de acceso, se han convertido en un producto ilícito en los mercados cibernéticos clandestinos.

[34]Antiguamente Mancomunidad Británica de Naciones (British Commonwealth of Nations), es una organización compuesta por 52 países soberanos. Su principal objetivo es la cooperación internacional en el ámbito político y económico, y desde 1950 la pertenencia a ella no implica sumisión alguna a la Corona británica. The Commonwealth, 2002. (i) Computer and Computer Related Crimes Bill and (ii) Model Law on Electronic Evidence (Commonwealth Model Law). En julio de 2000, la Secretaría del Commonwealth convocó una reunión del grupo de expertos para preparar las instrucciones de redacción de una ley modelo sobre delitos informáticos.

[35] Greenblatt, Sara, op. cit., nota 3, p. *vi*: International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU), 2010. Model Legislative Texts on Cybercrime/e-Crimes and Electronic Evidence (ITU/CARICOM/CTU Model Legislative Texts). Las tecnologías de la información y la comunicación están configurando el proceso de globalización. Reconociendo su potencial para acelerar la integración económica de la región del Caribe y, por lo tanto, su mayor prosperidad y transformación social, el Mercado Único y la Economía de la Comunidad del Caribe ha desarrollado una estrategia de TIC centrada en el fortalecimiento de la conectividad y el desarrollo.

Para entender "lo que hacen los hackers", recapitularemos e ilustraremos las técnicas y procedimientos más populares en uso.

Ping-of-Death Attack Against Web Servers: Ataque de Ping-of-Death contra servidores Web, el término PING (Internet de paquetes) se refiere a un método para determinar si un sistema está presente en una red y está funcionando correctamente. Para realizar un ping, se utiliza un ICMP (protocolo de mensajes de control de Internet) para escanear o probar una conexión y localizar accesos de red.

Las redes utilizan ICMP para identificar y localizar problemas; por ejemplo, un enrutador que no puede conmutar paquetes de datos a la misma velocidad que los recibe. Los mensajes ICMP se utilizan para comunicar mensajes entre sistemas de forma completamente automática. Cuando, por ejemplo, un usuario pings un servidor, está enviando al servidor un paquete de información. Si el servidor está en la red, enviará un paquete de respuesta. Sin embargo, si un servidor recibe muchos paquetes en un corto espacio de tiempo (flujo de paquetes), puede llegar a fluir con información a una velocidad tal que ya no puede responder, bloquear y detener a usuarios legítimos de descargar información.

Negación de servicio (DoS): Los script-kiddies que trabajan contra grandes corporaciones y compañías suelen llevar a cabo estos ataques. Estos son ataques altamente distribuidos que requieren el uso de muchas computadoras, llamadas zombies, porque se usan sin el conocimiento de sus propietarios y administradores. Estos sistemas vulnerables, como los pertenecientes a las universidades, se transforman en zombies y se utilizan como bases de lanzamiento para llevar a cabo ataques DoS con el uso de software malicioso previamente instalado. [36]

La penalización de estos medios comisivos se enfrenta a una serie de retos, entre los que cabe mencionar, el nexo causal entre la preparación y la tentativa de un delito, así como el problema de su ambivalencia de su uso, ya que pueden utilizarse para fines legales o criminales. No obstante, existen precedentes en el control de la delincuencia con la criminalización de objetos conocidos como *herramientas de robo*, y de esta forma, los instrumentos legales multilaterales de cibercrimen han tipificado delitos. Por ejemplo, en el Informe explicativo de la Convención sobre el Delito Cibernético del Consejo de Europa se señala que el objeto de la penalización de las herramientas de uso indebido en la computadora, es prevenir los actos que preceden a delitos como el *hacking* y además evitar la creación de mercados clandestinos. Con el fin de evitar la doble penalización de la posesión dudosa o la posesión con fines legítimos de herramientas informáticas de uso indebido, los instrumentos internacionales y regionales suelen requerir una

[36] Chiesa, Raoul, op. cit. nota 33, p.138

intención específica de uso para los fines de un delito, es decir, el elemento subjetivo específico.

Los instrumentos multilaterales de ciberdelincuencia incluyen disposiciones relativas a dos tipos de herramientas informáticas de mal uso: i) software y hardware; y ii) contraseñas y códigos que permitan el acceso a sistemas informáticos y datos. Nueve instrumentos multilaterales de ciberdelincuencia exigen sanciones tanto del software como de los códigos. Sin embargo, un buen instrumento normativo (v.gr. el Acuerdo de la Comunidad de Estados Independientes) requiere la tipificación tanto del uso como la distribución de software malicioso, excluyendo así el hardware y los códigos del objeto material del delito.

Actualmente, los perpetradores están cifrando o encriptando cada vez más sus mensajes. Los organismos encargados de hacer cumplir la ley señalan que los infractores están utilizando tecnología de cifrado para proteger la información almacenada en sus discos duros, lo que dificulta gravemente las investigaciones criminales. Además de una amplia penalización de los actos relacionados con la pornografía infantil, en la actualidad se están debatiendo otros enfoques, como la aplicación de obligaciones dirigidas a proveedores de servicios de Internet, para registrar usuarios o bloquear o filtrar el acceso a sitios web relacionados con la pornografía infantil.

La Convención de Budapest clasifica en su artículo 6, las herramientas de uso indebido de la computadora.

> *Artículo 6 - Abuso de los dispositivos.*
>
> *1 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:*
>
> *a) la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:*
>
> *i) un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;*
>
> *ii) una contraseña, un código de acceso o datos informáticos similares que permitan*

tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b) la posesión de alguno de los elementos contemplados en los anteriores apartados a): i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2 No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3 Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a): ii) del presente artículo.

Mientras que en los Estados parte de la Convención de Budapest consideran tipificado esta conducta relacionada con el *Abuso de los dispositivos,* la legislación mexicana no contiene en su marco jurídico federal ningún tipo penal que pudiera sancionarla.

3.1.5. Fraude relacionado con la informática

Hasta aquí, el bien jurídico protegido en los crímenes contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos es la integridad de la información de la computadora y los propios datos. Por el contrario, las disposiciones penales sobre el fraude y la falsificación relacionados con la informática, tutelan los bienes jurídicos como la propiedad, los activos financieros y la autenticidad de los documentos.

El fraude informático es uno de los delitos más populares en Internet, ya que permite al infractor utilizar herramientas de automatización y software para enmascarar las identidades de los criminales. La automatización permite a los delincuentes obtener grandes beneficios de una serie de pequeños actos. Una estrategia utilizada por los delincuentes es asegurar que la pérdida financiera de

cada víctima sea inferior a un cierto límite. Con una pérdida pequeña, las víctimas son menos propensas a invertir tiempo y energía en informar e investigar tales crímenes.

> *Estos implican el uso de la computadora para cambiar registros, para hacer transferencias monetarias, o para victimizar a las empresas. Muchos de estos tipos de delitos son cometidos por empleados o antiguos empleados. En algunos casos, una empresa puede estar involucrada en actividades fraudulentas.*[37]

Aunque estos delitos se llevan a cabo utilizando la tecnología informática, la mayoría de las legislaciones penales, los clasifican no como delitos informáticos, sino como fraude genérico. La principal distinción entre el fraude informático y el genérico es el blanco del fraude. Si los delincuentes tratan de influir en una persona, la ofensa es generalmente reconocida como fraude. Cuando los infractores se dirigen a sistemas informáticos o de procesamiento de datos, las infracciones suelen clasificarse como fraude informático. Los delitos de fraude informático más comunes incluyen el fraude de subastas en línea y el fraude por adelantado.

Las subastas en línea ahora son uno de los servicios de comercio electrónico más populares; eBay es el mayor mercado de subastas en línea del mundo, donde compradores pueden acceder a productos de nicho variados o especializados, además de disfrutar de una audiencia mundial, estimulando la demanda y aumentando los precios. Los delincuentes que cometen delitos sobre plataformas de subastas pueden aprovechar la ausencia de contacto cara a cara entre los vendedores y los compradores. La dificultad de distinguir entre usuarios genuinos y delincuentes ha dado lugar a que el fraude de subastas sea uno de los más populares de los delitos cibernéticos. Los dos métodos más comunes incluyen, por un lado la oferta de bienes inexistentes, y solicitar a los compradores a pagar

[37] W. Osterburg, James and H. Ward, Richard, *Criminal investigation a method for reconstructing the past,* Sixth Edition, AP Anderson publishing, NJ 2010, p.497 "A growing number of what may be described as "lower-level" crimes are being reported. These involve use of the computer to change records, to make monetary transfers, or to victimize companies. Many of these types of crime are committed by employees or former employees. In some cases, a company itself may be involved in fraudulent activity"

antes de la entrega y por otro, la compra de bienes y pidiendo la entrega, sin la intención de pagar.

En el fraude por adelantado, los infractores envían correos electrónicos pidiendo ayuda a los destinatarios en la transferencia de grandes cantidades de dinero a terceros y les prometen un porcentaje, si aceptan procesar la transferencia con sus cuentas personales. Los infractores luego les piden que transfieran una pequeña cantidad para validar sus datos de cuenta bancaria, basados en el sistema similar a la lotería, donde los encuestados pueden estar dispuestos a erogar en una pequeña pero cierta pérdida, a cambio de una ganancia grande pero improbable. Una vez que transfiere el dinero, nunca vuelven a saber de los delincuentes. Si envían su información de cuenta bancaria, los infractores pueden usar esta información para actividades fraudulentas. Las investigaciones europeas muestran que, a pesar de diversas campañas e iniciativas de información, los fraudes por pagos por adelantado siguen creciendo.

En el Código Penal Federal se toca el tema del fraude en su numeral 386, donde, bien podría encajar el delito de fraude informático porque no distingue el medio por el cual se realiza el engaño ni la forma en que cae en el error, por tanto considero que este tipo penal subsume parcialmente el fraude realizado a través de la internet, porque no hay que olvidar que lo que se lesiona es el patrimonio como bien jurídico tutelado, y quedaría sin tipificar la conducta que lesiona el patrimonio a través de la pérdida de información virtual.

> *Artículo 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.*

En este orden de ideas la Convención de Budapest sobre ciberdelincuencia establece la siguiente directriz para los Estados parte incluyendo a México, para definir el medio comisivo.

> *Artículo 8 - Fraude informático*
>
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen*

un perjuicio patrimonial a otra persona mediante:

a) cualquier introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

3.1.6. Falsificación relacionada con la informática

La falsificación relacionada con la computadora describe la manipulación de documentos digitales. El delito puede, por ejemplo, ser cometido mediante la creación de un documento que aparentemente se origina en una institución confiable que manipula imágenes electrónicas o que altera documentos de texto. Asimismo, la falsificación de correos electrónicos es un elemento esencial del phishing[38] (suplantación de identidad), que es un serio desafío para el legislador en todo el mundo, porque el phishing busca hacer que los usuarios divulguen información personal y secreta ya que los delincuentes envían correos electrónicos que parecen comunicaciones de instituciones financieras legítimas y diseñados de tal forma que es difícil para los clientes identificarlos como e-mails falsos. Así, el correo electrónico pide al destinatario que revele o divulgue cierta información confidencial, lo que permite a los infractores hacer transferencias o fraude a través de internet con esa información.

Los delincuentes siempre han manipulado información de documentos con falsificaciones digitales, porque tales documentos actualmente se pueden copiar sin pérdida de calidad y se pueden manipular fácilmente. Para los expertos forenses, es difícil probar manipulaciones digitales, a menos que exista la técnica adecuada para proteger un documento en riesgo de ser falsificado.

El marco normativo relativo a la falsificación informática suele requerir dos elementos necesarios: a) la alteración o manipulación de datos informáticos, y b) una intención específica de utilizar los datos como si fueran auténticos. Varios

[38] Gercke, Marco, *Understanding cybercrime: phenomena, challenges and legal response*. *The ITU Telecommunication Development Bureau Publication*. September 2012, p.18

países de Europa, por ejemplo, han cubierto la falsificación relacionada con la informática al ampliar la definición de *documento* para usar *datos informáticos*. Otros países aplican disposiciones generales a la falsificación informática sin modificar la legislación si las disposiciones tradicionales de falsificación pueden interpretarse en el sentido de que incluyen documentos digitales, firmas y datos.

Mientras la Convención sugiere tipificar como delito la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, como si se tratara de datos auténticos.

> *Artículo 7 - Falsificación informática*
>
> *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.*

En el derecho mexicano y en específico el Código Penal Federal en su artículo 239, sólo prevé la falsificación de documentos en forma material, no de manera virtual como lo sugieren los datos informáticos.

> *Artículo 239.- Al que cometa el delito de falsificación de títulos al portador y documentos de crédito público, se le impondrán de cuatro a diez años de prisión y multa de doscientos cincuenta a tres mil pesos.*

3.1.7. Delitos de robo de identidad

La conectividad global, la automatización del procesamiento de datos y el desarrollo de transacciones que no son de cara a cara han generado mayores oportunidades para el robo de información relacionada con la identidad y datos personales a través de sistemas informáticos[39]. Este delito se dirige tanto a la sustracción de información de identificación personal, como a otros tipos de

[39] Greenblatt, Sara, op. cit., nota 3, p.99.

información de identificación, incluyendo los números de tarjetas de crédito, la información de cuentas bancarias, los números de pasaporte o de la licencia de conducir, las cuentas de Internet, las contraseñas, las direcciones IP, etcétera.

> *El robo de identidad toma muchas formas, el más común de los cuales está relacionado con varios tipos de fraude, robo y tergiversación. La actividad criminal puede variar desde usos únicos o múltiples de tarjetas de crédito hasta esquemas elaborados que resultan en pérdidas que ascienden a cientos de miles de dólares.*[40]

Esta información puede ser objeto de varios actos constitutivos de robo de identidad, incluyendo la obtención, la transferencia y el uso de la misma. Los medios de obtención pueden ser a través del acceso ilegal a los sistemas informáticos, mediante el uso de programas maliciosos, mediante el uso de phishing o suplantación de identidad, o mediante la adquisición ilegal de datos informáticos provenientes de los mismos empleados corporativos.

> *El phishing es una estafa informática en la que se contacta a una víctima por correo electrónico o, en algunos casos, por teléfono, y se le solicita su número de seguro social u otra información confidencial que pueda ser utilizada para proteger tarjetas de crédito, cuentas abiertas , o usar la información para defraudar a la víctima.*
>
> *La suplantación (Spoofing) implica esfuerzos de criminales para obtener números de identificación de llamadas para el teléfono celular de la víctima, los cuales pueden usarse para obtener información sobre la identidad de la víctima. En 1996, la Federal Trade Commission (FCC) presentó el primer caso contra una compañía hipotecaria que supuestamente utilizó la información para el telemarketing. Ha habido una proliferación de empresas que venden los llamados "SpoofCards" como tarjetas telefónicas, que pueden ser utilizadas por los perpetradores para presentar como bancos u otras organizaciones. Aunque la venta de SpoofCards es legal en la mayoría de los estados,*

[40] W. Osterburg, James op. cit, nota 33, p.495 “Identity theft takes many forms, the most common of which is related to various types of fraud, theft, and misrepresentation. Criminal activity may range from single or multiple uses of credit cards to elaborate schemes resulting in losses amounting to hundreds of thousands of dollars”

estas tarjetas pueden proporcionar a los criminales información sensible.[41]

El término robo de identidad, describe el acto delictivo de obtener fraudulentamente y usar la identidad de otra persona[42]. Estos actos pueden llevarse a cabo con la ayuda de medios técnicos, en línea mediante el uso de la tecnología de internet. En general, el delito descrito como robo de identidad contiene tres fases diferentes. En la primera fase, el delincuente obtiene información relacionada con la identidad, la cual puede ser llevada a cabo, con el uso de software malicioso o ataques de phishing como ya se dijo; la segunda fase se caracteriza por la manipulación de la información relacionada con la identidad para destinarla al uso de las conductas delictivas y la tercera fase, es en sí la ejecución del uso de la información relacionada con la identidad en un delito específico. En la mayoría de los casos, el acceso a los datos relacionados con la identidad permite al perpetrador cometer varios delitos. Lo importante es no centrarse en el conjunto de datos o información, sino en la capacidad de utilizar éstos en actividades delictivas. Ejemplos de tales delitos pueden ser la falsificación de documentos de identificación o el fraude con tarjetas de crédito. *El haber tenido un acceso no autorizado al ordenador de una persona y con sus contraseñas haber hecho el fraude en sus cuentas de banco o alteración de otra información personal*.[43]

En México, el delito de robo de identidad va en aumento día con día, según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos[44], el robo de identidad se da por la pérdida de documentos, por el robo de carteras y portafolios, y por información tomada directamente de una tarjeta bancaria. Comúnmente, el delito de robo de identidad se usa de manera ilegal para abrir cuentas de crédito, contratar líneas telefónicas,

[41] Íbidem, p.496
[42] Gercke, Marco, op. cit., nota 18, p.31.
[43] Huerta Estefan, Janet, "Frente a la Cibercriminalidad más que buenas leyes se requiere prevención: Javier Fernández Teruelo", *Revista Foro Jurídico*, México, Núm. 165, junio 2017, p.9
[44] CONDUSEF, "Robo de identidad" *Categoría: Revista Proteja su Dinero*. Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad. Fecha de Consulta 19 de Julio 2017. 12:57.

seguros de vida, realizar compras e incluso, en algunos casos, para el cobro de seguros de salud, vida y pensiones.

Desafortunadamente la tipificación en el Código Penal federal aún está en espera debido a que desde el 29 de Noviembre de 2016 que la Cámara de Diputados aprobó, el dictamen que adiciona un artículo 430 al Código Penal Federal, para sancionar la usurpación de identidad con una pena de uno a seis años de prisión y 400 a 600 días de multa y, en su caso, la reparación del daño que se hubiere causado, el cual fue enviado al Senado de la República para sus efectos constitucionales y que no se ha concretado[45]. El dictamen contempla el siguiente tipo:

> *…quien por sí o por interpósita persona, usando cualquier medio lícito o ilícito, se apodere, apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o, bien, suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión.*
>
> *Las penas aumentarán hasta en una mitad cuando el ilícito sea cometido por un servidor público que, aprovechándose de sus funciones, tenga acceso a bases de datos que contengan este tipo de información, así como a los particulares responsables del tratamiento de datos personales sensibles, en términos de la ley en la materia.*

3.1.8. Delitos de copyright o marcas registradas

La materia de derecho de propiedad intelectual es algo más amplio que los instrumentos internacionales y regionales sobre ciberdelincuencia. Los principales actores e instrumentos son la Organización Mundial del Comercio[46] y el Acuerdo

[45] Boletín N°. 2661. Delito de usurpación de identidad será castigado con uno a seis años de prisión. http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Boletines/2016/Noviembre/29/2661-Delito-de-usurpacion-de-identidad-sera-castigado-con-uno-a-seis-anos-de-prision. Fecha de consulta 20 de Julio de 2017, 14:38.

[46] La Organización Mundial del Comercio (OMC) es la única organización internacional que se ocupa de las normas que rigen el comercio entre los países. Los pilares sobre los que descansa son los Acuerdos de la OMC, que han sido negociados y firmados por la mayoría de los países que participan en el comercio mundial y ratificados por sus respectivos Parlamentos. El objetivo es

sobre los ADPIC[47], que por primera vez incluye disposiciones penales a nivel internacional en materia de violaciones de derechos de autor comerciales, así como el Tratado sobre Derecho de Autor de la Organización Mundial de la Propiedad Intelectual[48] (OMPI). Más recientemente, el Acuerdo Comercial de Lucha contra la Falsificación[49] (ACTA) tenía por objeto consolidar las disposiciones penales sobre la falsificación ilícita de marcas o los derechos de autor o relacionados con la piratería a escala comercial.

Con el cambio de analógico a digital, la digitalización ha permitido a la industria del entretenimiento agregar características y servicios adicionales a películas en DVD, incluyendo idiomas, subtítulos, trailers y material adicional. CDs y DVDs han demostrado ser más sostenibles que los discos y cintas de video. También la digitalización ha abierto la puerta a nuevas violaciones de derechos de autor más rápida y precisa. Antes de la digitalización, copiar un registro o una cinta de vídeo siempre daba lugar a un grado de pérdida de calidad. Hoy en día, es posible duplicar fuentes digitales sin pérdida de calidad. Las infracciones de derechos de autor más comunes incluyen el intercambio de canciones protegidas por derechos de autor, archivos y software en sistemas de intercambio de archivos o mediante servicios de *share hosting*[50] y la elusión de los sistemas de gestión de derechos digitales (DRM).

---

garantizar que los intercambios comerciales se realicen de la forma más fluida, previsible y libre posible.

[47] El Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC o, en inglés, TRIPS), es el Anexo 1C del Convenio por el que se crea la OMC firmado en 1994. En él se establece una serie de principios básicos sobre la propiedad intelectual tendientes a armonizar estos sistemas entre los países firmantes y en relación al comercio mundial.

[48] La Organización Mundial de la Propiedad Intelectual (OMPI) es un organismo especializado del Sistema de Naciones Unidas, con sede en Ginebra Suiza, creado en 1967 con la firma de la Convención de Estocolmo. La OMPI está dedicada a fomentar el uso y la protección de las obras del intelecto humano.

[49] ACTA (del inglés Anti-Counterfeiting Trade Agreement, traducido como Acuerdo comercial anti-falsificación) es un acuerdo multilateral voluntario que propone fijar protección y respaldo a la propiedad intelectual, con el propósito de evitar la falsificación de bienes, los medicamentos genéricos y la piratería en Internet.

[50] Gercke, Marco, op. cit., nota 16, p. 28. Se refiere a un servicio de alojamiento web donde muchos sitios web residen en un servidor web conectado a Internet. Ésta es generalmente la opción más económica para el recibimiento, pues el coste total del mantenimiento del servidor se amortiza sobre muchos clientes.

Las violaciones de marcas registradas, son similares a las violaciones de derechos de autor. Los delitos relacionados con las marcas se han transferido al ciberespacio, de los cuales los más graves incluyen el uso de marcas en actividades delictivas con el objetivo de engañar a los usuarios y los delitos relacionados con nombres de dominio. Los sistemas de intercambio de archivos, permiten a los usuarios compartir archivos con millones de otros usuarios. Con sólo instalar el software de uso compartido de archivos, los usuarios pueden compartir y descargarlos de cientos de fuentes. Los sistemas de intercambio de archivos se pueden utilizar para intercambiar cualquier tipo de datos informáticos, incluyendo música, películas y software.

> *El cracking de software, o la piratería de software, consiste en crear scripts que pueden romper o romper los códigos de copyright de software protegido por derechos de autor. Para ello, las galletas deben registrar en primer lugar cada momento en el que la aplicación interactúa con el sistema de grabación para deducir dónde se encuentra la protección contra la piratería. Sobre la base de esta información, deben realizar un examen detallado del código para eliminar la protección.*
>
> *Es posible romper todo tipo de software: juegos, profesionales*
>
> *aplicaciones, códigos de fuente de sistemas operativos inéditos, lenguajes de scripting, herramientas phreaking y cracking, software para hacer funcionar BBSs, etc. Una vez que se agrietó, el software protegido se mantiene generalmente en directorios ocultos, sí mismos. Sólo las personas de confianza pueden tener acceso a ellas. El software pirateado también se mantiene en BBSs y es generalmente descargable gratuitamente. A veces, sin embargo, el acceso a estos BBS requiere el pago de una tarifa para cubrir los gastos de gestión. Dependiendo del tamaño de la donación, es posible pasar de un acceso limitado a un acceso total.*[51]

Sin embargo, la tecnología de intercambio de archivos no sólo es utilizada por personas comunes y criminales, sino también por negocios regulares. Consecuentemente, el uso de sistemas de intercambio de archivos plantea desafíos para la industria del entretenimiento porque no está claro hasta qué punto las caídas en las ventas de CD / DVD, entradas de cine, copias de películas que incluso han aparecido en los sistemas de intercambio de archivos antes de que fueran lanzadas oficialmente en cines. Ahora con el desarrollo de sistemas

[51] Chiesa, Raoul, op. cit. nota 31, p.170, “Bulletin board systems (BBSs) are electronic bulletins that contain download areas where you can download suggestions and software (games, cracking tools, etc.) and fi nd chats and discussion forums”.

anónimos de intercambio de archivos se dificulta el trabajo de los titulares de derechos de autor, así como el de los organismos encargados de hacer cumplir la ley.

Por todo lo anterior, muchos Estados involucran medidas de Derecho Civil, para reclamaciones de daños y el derecho a la información, lo que obliga a los proveedores de servicios de Internet a registrar las direcciones IP de los infractores de los derechos de autor, a enviar avisos de advertencia a los infractores de primera vez y asumir la responsabilidad de sancionar a los infractores reincidentes o colaborar notificando a los titulares o autoridades.[52]

Los delitos relacionados con el dominio URL, se relacionan por un lado, con el *cybersquatting* o ciberocupación, el cual es el procedimiento ilegal de registro de un nombre de dominio idéntico o similar a la marca de un producto o una empresa. En la mayoría de los casos, los infractores venden el dominio a un alto precio a la empresa lo utilizan para vender productos o servicios engañosos a los usuarios a través de su supuesta conexión con la marca.

3.1.9. Correo no deseado o spam

Un número significativo de todos los correos electrónicos que se envían son SPAM. Como consecuencia, varios países, así como las recientes leyes modelo, han incluido disposiciones que tipifican como delito los actos relacionados con la distribución de SPAM. Un término clave utilizado en dicha disposición es el *correo electrónico múltiple*. El término SPAM se relaciona a cosas que por su abundancia son indeseables y que a fin de cuentas representan basura informática, como es el caso de correos electrónicos que contienen información que en su mayoría es comercial que no se ha pedido, relacionada con productos o servicios. Pero no sólo es exclusivo de los correos electrónicos, sino que pueden ser enviados a través de mensajes, foros, blogs, teléfonos móviles, grupos de noticias, etcétera.

[52] Greenblatt, Sara, op. cit., nota 3, p. 105.

> *Todos recibimos SPAM y lo encontramos bastante irritante y quizás incluso asqueroso cuando se adjuntan sitios pornográficos a estos correos electrónicos, pero en su mayor parte, estas comunicaciones por correo electrónico no son vistas como amenazas o acoso. Sin embargo, las comunicaciones podrían convertirse en acecho si persisten y si los mensajes amenazantes los acompañan, y por lo tanto deben ser observados atentamente*[53]

Sin embargo la situación se agrava cuando se oferta pornografía, productos para la salud no controlados por la secretaría de salud, la piratería, la educación sin reconocimiento oficial de la secretaría de educación, entre otros. Además los correos pueden venir acompañado con archivos que contienen virus informáticos o código malicioso (malware[54]).

Los tipos de malware más comunes están: *Spyware*, el cual puede espiar y guardar registro de los sitios web que se consultan para después informar al creador del código; *Virus, Troyanos y Gusanos*, los cuales pueden usar la computadora como centro de envío de correos basura o utilizarla para atacar a otros usuarios o sitios de internet, es decir la convierten en un botnet, además de que destruyen información contenida en la misma; *Backdoors*, abre un puerto de la computadora para que el autor del malware pueda controlarlo, instalar otros códigos y utilizar más recursos del equipo; *Dialers*, hacen llamadas a números por cobrar con cargo al recibo del usuario; *Keyloggers*, registran todo lo capturado con el teclado lo almacenan en archivos ocultos para luego enviarlos al creador del malware.

> *Los programas malignos, como virus, gusanos y caballos de Troya, se dirigen a la computadora o al software de la computadora con la intención de dañar la computadora.*
>
> *Los virus son códigos maliciosos incrustados en programas o correos electrónicos que dañan el hardware o el software de la computadora.*
>
> *El gusano es un código que puede dañar los archivos y programas informáticos o*

[53] Moriarty, Laura, *Controversies in Victimology*, Second Edition, Matthew Bender & Company, Inc.,2008, p.104.

[54] El malware (del inglés “malicious software”), también llamado badware, código maligno, software malicioso, software dañino o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. Malware: backdoor o puerta trasera, drive-by downloads, rootkits, troyanos, Spyware, Adware, Hijacking, Keyloggers, Stealers, Dialers, Botnets, Rogue software y Ransomware.

disminuir el rendimiento de la computadora; es entregado por otro programa o aplicación, generalmente vía correo electrónico. Los virus y los gusanos fueron entregados originalmente por medios extraíbles, pero ahora se pueden encontrar en correos electrónicos, adjuntos de correo electrónico y programas gratuitos disponibles a través de Internet. Los virus y gusanos también se han encontrado incrustados en imágenes.

Los caballos de Troya son programas colocados en una computadora para capturar y enviar información a un tercero desconocido para el usuario de la computadora. Se han utilizado en casos de robo de identidad. Otro tipo de caballo de Troya captura la información de acceso de teclado del usuario y busca información personal y financiera.[55]

El filtrado de correo basura es una prioridad importante de todos los proveedores de correo electrónico debido al alto volumen de mensajes de spam enviados y recibidos todos los días. Los medios por los que se filtra el spam son variados y complejos, incluyendo el análisis del origen de los correos electrónicos para identificar fuentes conocidas de spam, así como análisis textual para identificar frases y patrones de contenido comunes en los mensajes. Los mensajes identificados como spam a veces se descartan por completo o se envían a las *carpetas de spam* del usuario. Además del filtrado de spam, los ISP también pueden desempeñar un papel en la lucha contra el tráfico malicioso, como el generado por botnets. De esta manera cuando los ISP son notificados, o identifican a partir de los patrones de tráfico de Internet, que una máquina en su red parece ser parte de una botnet o está infectada con software malicioso, una opción es bloquear parte o la totalidad del tráfico de esa dirección. Estas notificaciones pueden provenir de empresas de seguridad que controlan botnets, utilizando técnicas tales como máquinas *honeypot*[56] que deliberadamente traen software malicioso. Los ISP también pueden tomar medidas para identificar de forma anticipada las máquinas comprometidas, supervisando el tráfico de firmas conocidas, aunque se requiere cierto grado de segmentación para que esto sea efectivo. Una revisión emitida por la Agencia Europea de Seguridad de las Redes

[55] E. Douglas, John, et al, *Crime classification manual, a standard system for investigating, and classifying violent crimes*, Second Edition, John Wiley & Sons, Inc. San Francisco, CA, 2006, p.384

[56] Un honeypot, o sistema trampa o señuelo, es una herramienta de la seguridad informática dispuesto en una red o sistema informático para ser el objetivo de un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

y de la Información concluyó que: *Identificar el tráfico de botnet entre el tráfico benigno y regular es como buscar una aguja en 100 millones de pajares*. Tal como se mencionó con anterioridad, el monitoreo de tráfico también puede bajo ciertas circunstancias, entrar en conflicto con las leyes de protección de datos y privacidad.

3.1.10. Racismo y Xenofobia

A raíz de las negociaciones sobre el texto de la Convención sobre Cibercriminalidad, en Budapest el 23 de noviembre de 2001, resultó que la penalización del racismo y la distribución de material xenófobo eran cuestiones particularmente controvertidas. El racismo y la xenofobia en las TIC significa la distribución de imágenes, escritos o de cualquier otra representación de ideas o teorías que promuevan el odio, la discriminación o la violencia contra una persona o grupo de personas por motivos de raza, color, ascendencia u origen nacional o étnico o la misma religión, o que sirven de pretexto para promover el racismo y la xenofobia. No obstante en países con una fuerte protección constitucional a la libertad de expresión, el discurso de odio no es penalizado; las prohibiciones se pueden encontrar especialmente en África y Europa.

De manera genérica se puede decir que una de las formas más notables de discriminación es aquella, llamada xenofobia, que se hace contra las personas ajenas al grupo nacional o étnico por el mero hecho de serlo, y que es particularmente intensa por motivos raciales, lo que llamamos racismo.

Los instrumentos sobre la libertad de expresión como por ejemplo, la Primera Enmienda a la Constitución de los Estados Unidos, explican por qué ciertos actos de racismo no fueron penalizados por la Convención sobre Delitos Cibernéticos de

Budapest, pero su penalización fue incluida en el *Primer Protocolo Adicional, de Estrasburgo, 28.I.2003.*[57]

Primer Protocolo Adicional, No. 4. Protocolo Adicional a la Convención sobre Ciberdelincuencia, relativo a la penalización de actos de carácter racista y xenófobo cometidos a través de sistemas informáticos.

> *Artículo 2 - Definición*
>
> *1 A efectos del presente Protocolo, se entenderá por: "Material racista y xenófobo", todo material escrito, cualquier imagen o cualquier otra representación de ideas o teorías, que aboga, promueve o incita al odio, discriminación o violencia, contra cualquier individuo o grupo de individuos, basado en la raza, color, ascendencia u origen nacional o étnico, así como religión, si éste se utiliza como pretexto para cualquiera de estos conductas.*
>
> *2 Los términos y expresiones utilizados en el presente Protocolo se interpretarán de la misma manera que se interpretan en el marco de la Convención.*

Así mismo, establece las medidas que deben tomarse por los Estados y del que México es parte desde el 2014.

> *Artículo 3 - Difusión de material racista y xenófobo a través de sistemas informáticos*
>
> *1 Cada parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos penales en su derecho interno, cuando se cometan intencionalmente y sin derecho, las siguientes conductas: distribución o puesta a disposición del público de material racista y xenófobo a través de un sistema informático.*
>
> *2 Cada parte podrá reservarse el derecho de no atribuir responsabilidad penal a la conducta definida en el párrafo 1 de este artículo, cuando el material, tal como se define en el párrafo 1 del artículo 2, abogue, promueva o incita a la discriminación que no esté asociada con el odio o la violencia, siempre que se disponga de otros recursos efectivos.*

3.1.11. Pornografía infantil

Prácticamente todas las imágenes que contienen pornografía infantil se transmiten por la web, a través de intercambios bilaterales y multilaterales. Los bienes jurídicos protegidos por la penalización de la pornografía infantil incluyen la protección de los menores contra los abusos y la prohibición de los mercados de

[57] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Strasbourg, 28.I.2003 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189. Consulta 20 de Julio 2017, 18:00.

las imágenes pornográficas infantiles. Aunque los marcos internacionales demuestran muchas similitudes con respecto a la penalización de la pornografía infantil, las diferencias también se relacionan con el objeto, la edad de los niños y los actos cubiertos. *Se estima que la pornografía infantil en Internet genera USD 2,500 millones anualmente en todo el mundo*.[58]

El contenido sexualmente relacionado, fue uno de los primeros elementos que se distribuyeron comercialmente a través de Internet, lo que ofrece acceso a los minoristas de material erótico y pornográfico, incluyendo el intercambio de medios, como imágenes, películas, cobertura en vivo, sin necesidad de un envío costoso; asimismo, este acceso a nivel mundial, facilita el incremento de un número significativamente mayor de clientes en comparación con las tiendas minoristas. El internet se ve a menudo como un medio anónimo, aspecto que los consumidores de la pornografía aprecian. Investigaciones recientes[59] han identificado hasta 4,2 millones de sitios web pornográficos que pueden estar disponibles en Internet en cualquier momento. Además de los sitios web, el material pornográfico puede distribuirse a través de sistemas de intercambio de archivos y sistemas de mensajería instantánea que también están disponibles en internet.

> *Internet hace factible la consulta de páginas web con material pornográfico, pero mantiene al usuario en el anonimato. Los programas "peer to peer" hacen posible compartir el material ubicado en el disco duro de las computadoras, sin dejar rastro. El correo electrónico permite enviar fotografías o videos de una punta del mundo a la otra en cuestión de segundos, sin correr el riesgo de pasar por aduanas o controles policiales. Los chats, foros y páginas de comunidades facilitan la comunicación entre pedófilos e incluso el contacto directo con menores.*[60]

Internet se ha convertido en un canal privilegiado para la distribución de pornografía infantil ya que en los años setenta y ochenta, el mercado comercial de pornografía infantil se concentraba principalmente en Europa y Estados Unidos y

[58] TopTenReviews es un sitio web que recopila reseñas de álbumes de música, videojuegos, películas, software, hardware, DVD y otras publicaciones. http://www.toptenreviews.com/.
[59] Gercke, Marco, op. cit., nota 38, p.22.
[60] Téllez Valdés, Julio, *Derecho informático*, cuarta edición, Editorial Mc Graw Hill, México, 2009, p.197.

su producción era local, su acceso era caro y difícil de obtener de tal suerte que al comprar o vender pornografía infantil tenía aparejada una serie de riesgos que ya no existen en la actualidad, o al menos no en cierto grado. La disponibilidad de cámaras de vídeo y el acceso a nuevas tecnologías facilitó en gran medida la producción de material pornográfico.

El acceso a la pornografía infantil también representaba muchos riesgos para el delincuente porque en los años noventa, la pornografía infantil era principalmente transportada a través de los servicios postales, y las investigaciones exitosas llevaron a la detección de un número significativo de delincuentes. En opinión de los expertos, la policía estaba en esa época en condiciones de hacer frente a los desafíos que implicaban estas conductas. Pero la situación cambia drásticamente con la disponibilidad de aplicaciones de intercambio de datos basados en Internet.

Mientras que en el pasado, la aplicación de la ley se enfrentó con material analógico, hoy en día la gran mayoría de material descubierto es digital. Desde mediados de la década de 1990, los infractores han recurrido cada vez más a servicios de red para la distribución de ese material. Los problemas resultantes en términos de detección e investigación de casos de pornografía infantil han sido reconocidos. El Internet es hoy el canal principal para el comercio regular de pornografía en general, así como de la pornografía infantil en particular.

Algunos países permiten el intercambio de material pornográfico entre adultos y limitan la criminalización a los casos en que los menores acceden a este tipo de material, tratando de protegerlos, pues el acceso a éste material podría influir negativamente en su desarrollo psicosexual. Sin embargo, otros países penalizan cualquier intercambio de material pornográfico incluso entre adultos, sin centrarse en grupos específicos. A diferencia de las opiniones divergentes sobre la pornografía de adultos, la pornografía infantil es ampliamente condenada y las conductas relacionadas con ésta son ampliamente reconocidas como actos delictivos. Las organizaciones internacionales se dedican a la lucha contra la pornografía infantil en línea, con varias iniciativas jurídicas internacionales, entre ellas: la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989,

la Decisión marco del Consejo de la Unión Europea de 2003 sobre la lucha contra la explotación sexual de niños y la pornografía infantil; y la Convención del Consejo de Europa de 2007 sobre la Protección de los Niños contra la Explotación Sexual y el Abuso Sexual, entre otros.

Dos factores clave en el uso de las TIC para el intercambio de pornografía infantil actúan como obstáculos para la investigación de estos delitos: 1) El uso de monedas virtuales y el pago anónimo, y 2) El uso de la tecnología de cifrado. Además de una amplia penalización de las conductas relacionadas con la pornografía infantil, en la actualidad se están debatiendo otros enfoques, como la aplicación de obligaciones en los servicios de Internet para registrar usuarios o bloquear o filtrar el acceso a sitios web relacionados con la pornografía infantil.[61]

Por otro lado, la Convención de Budapest se pronuncia al respecto de la pornografía infantil en su artículo 9 de la siguiente manera:

> *Artículo 9 - Delitos relacionados con la pornografía infantil*
>
> *1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:*
>
> *a) la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;*
>
> *b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;*
>
> *c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,*
>
> *d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;*
>
> *e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.*
>
> *2. A los efectos del anterior apartado 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:*
>
> *a) un menor comportándose de una forma sexualmente explícita;*
>
> *b) una persona que parezca un menor comportándose de una forma sexualmente explícita;*
>
> *c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.*
>
> *3. A los efectos del anterior apartado 2, por "menor" se entenderá toda persona menor de*

[61] Greenblatt, Sara, op. cit. nota 3, p.24

18 años. No obstante, cualquier parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.

4. Cualquier parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

El Código Penal Federal en su Libro Segundo y Titulo Octavo, de los delitos contra el libre desarrollo de la personalidad con relación al Capítulo II de la pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo, establece lo siguiente:

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

A quien fije, imprima, video grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participen una o varias personas menores de dieciocho años de edad o una o varias personas que no tienen capacidad para comprender el significado del hecho o una o varias personas que no tienen capacidad para resistirlo, se le impondrá la pena de siete a doce años de prisión y de ochocientos a dos mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito.

La misma pena se impondrá a quien reproduzca, almacene, distribuya, venda, compre, arriende, exponga, publicite, transmita, importe o exporte el material a que se refieren los párrafos anteriores.

Para la legislación mexicana, evidentemente no existe tipificación con respecto de esta conducta especificada como delito informático de pornografía infantil; no obstante, haciendo una interpretación sistemática, bien puede subsumirse esa conducta en el tipo penal, por tratarse un tipo general a la luz del principio de consunción, toda vez que a falta de norma especial, la más amplia absorbe para resolver el problema. Asimismo, se tiene el mismo caso de la Ley General Para Prevenir, Sancionar y Erradicar los delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos delitos en su artículo 16, primer

párrafo; que sí especifica la exhibición del material pornográfico a través de sistemas de cómputo, electrónicos o sucedáneos:

> *ARTÍCULO 16. Se impondrá pena de 15 a 30 años de prisión y de 2 mil a 60 mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales resultantes, al que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad, o que no tenga la capacidad de comprender el significado del hecho, o no tenga capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal, con fines sexuales, reales o simulados, con el objeto de producir material a través de video grabarlas, audio grabarlas, fotografiarlas, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos, y se beneficie económicamente de la explotación de la persona.*

3.1.12. Ciberterrorismo

El terrorismo amenaza la seguridad de una nación en todos los niveles, a saber, poniendo en peligro la seguridad física de los individuos y las comunidades, sembrando miedo y pánico; también menoscaba el estado de derecho, globalmente desestabiliza a los países y pone en peligro la paz sostenible; además tiene un impacto devastador en el comercio y otras actividades económicas, lo que a su vez perjudica el desarrollo.

> *Existen muchas definiciones de terrorismo que, desde el punto de vista de la investigación, carecen prácticamente de sentido porque son vagas y no proporcionan un corpus delicti claro para el crimen. A los efectos de este texto, el terrorismo puede definirse como el uso de la fuerza o el temor a la fuerza para lograr un fin político o criminal. Otra definición, ofrecida por el Equipo de Tareas del Vicepresidente para Combatir el Terrorismo, aporta algunas aclaraciones adicionales: [Terrorismo] es el uso ilegal o amenaza de violencia contra personas o bienes para promover objetivos políticos o sociales. Generalmente se pretende intimidar o coaccionar a un gobierno, individuos o grupos para modificar su comportamiento o políticas.*[62]
>
> *La amenaza terrorista es una estructura de red flexible y transnacional, habilitada por la tecnología moderna y caracterizada por una interconectividad libre dentro y entre grupos. En este ambiente, los terroristas trabajan juntos en la financiación, el intercambio de inteligencia, entrenamiento, logística, planificación y ejecución de ataques. Los grupos*

[62] W. Osterburg, James op. cit, nota 38, p.520 “There are many definitions of terrorism that, from an investigative standpoint, are virtually meaningless because they are vague and do not provide a clear corpus delicti for the crime. For purposes of this text, terrorism can be defined as the use of force or the fear of force to achieve a political or criminal end. Another definition, offered by the Vice President’s Task Force on Combating Terrorism, provides some further clarification: [Terrorism] is the unlawful use or threat of violence against persons or property to further political or social objectives. It is generally intended to intimidate or coerce a government, individuals or groups to modify their behavior or policies”

terroristas con objetivos en un país o región pueden obtener fuerza y apoyo de grupos de otros países o regiones[63].

Según la Agencia Central de Inteligencia de los Estados Unidos, las organizaciones terroristas operan en tres niveles; en el primer nivel están los terroristas que operan principalmente dentro de un solo país, su alcance es limitado, pero en este entorno global sus acciones pueden tener consecuencias internacionales. En el siguiente nivel están las organizaciones terroristas que operan regionalmente sus operaciones trascienden al menos una frontera internacional. Las organizaciones terroristas de alcance mundial forman la tercera categoría. Sus operaciones abarcan varias regiones y sus ambiciones pueden ser transnacionales e incluso globales. Estos tres tipos de organizaciones están unidas entre sí de dos maneras. En primer lugar, pueden cooperar directamente compartiendo inteligencia, personal, experiencia, recursos y refugios seguros. En segundo lugar, pueden apoyarse recíprocamente de manera menos directa, por ejemplo promoviendo la misma agenda ideológica y reforzando los esfuerzos de los demás para cultivar una imagen internacional favorable a su causa. Las organizaciones terroristas aprenden y comparten información obtenida de nuestros sitios web, explotan las vulnerabilidades de la infraestructura crítica de telecomunicaciones y se comunican a través de las mismas rutas de Internet abierto.

Después de los atentados del 9/11, fue lo que provocó el inicio de una intensa discusión sobre el uso de las TIC por parte de los terroristas. Esta discusión fue facilitada por informes de que los delincuentes utilizaron Internet para preparar el ataque. Aunque los ataques no fueron ataques cibernéticos, en la medida en que el grupo que llevó a cabo el ataque del 19/11 no realizó un ataque basado en internet, pero sí desempeñó un papel en la preparación de la ofensa.[64]

[63] Central Intelligence Agency, *National Strategy For Combating Terrorism*, National Security Strategy of the United States. February 2003. https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf Consulta 21 de julio 2017 18:00
[64] Gercke, Marco, op. cit., nota 38, p.34.

Hoy en día se sabe que los terroristas utilizan las TIC y el internet para: propaganda, recopilación de información, preparación de ataques en el mundo real, publicación de material de capacitación, comunicación, financiación del terrorismo, ataques contra infraestructuras críticas.

El Objetivo principal de la CIA para combatir el terrorismo estriba en lo siguiente: Establecer y mantener una norma internacional de responsabilidad en la lucha contra el terrorismo. Además de la presión estadounidense para poner fin al patrocinio estatal, apoyaremos fuertemente nuevos estándares estrictos para que todos los estados se reúnan en la guerra global contra el terrorismo. Estados que tienen derechos de soberanía. La RCSNU 1373[65] establece claramente las obligaciones de los Estados en la lucha contra el terrorismo.

No obstante, de no referir ninguna recomendación en la Convención de Budapest del 2001, recientemente, el mandato de la ONUDC en materia de prevención del terrorismo se reiteró en la resolución 70/177 de la Asamblea General sobre asistencia técnica para la aplicación de los convenios y protocolos internacionales relacionados con la lucha contra el terrorismo. La resolución adoptada el 17 de diciembre de 2015 pide a la ONUDC que siga prestando asistencia técnica a los Estados Miembros para la ratificación y la incorporación legislativa de los instrumentos jurídicos internacionales relacionados con el terrorismo y redoble sus esfuerzos para apoyar a los Estados Miembros en la lucha contra el terrorismo. Esto incluye los desafíos emergentes relacionados con la cooperación internacional en materia penal, los combatientes terroristas extranjeros y su radicalización, el creciente nexo entre la delincuencia organizada transnacional y el terrorismo y la destrucción del patrimonio cultural por terroristas, además de los trabajos en curso sobre delitos de terrorismo relacionados con el transporte, químico, biológico, radiológico y nuclear y de los derechos humanos en la lucha contra el terrorismo, entre otros.

[65] Resolution 1373 (2001). Adopted by the Security Council at its 4385th meeting, on 28 September 2001 (Resoluciones del Consejo de Seguridad relativas al terrorismo).

En la legislación mexicana el delito de terrorismo genérico, está previsto tanto en el título primero referente a los delitos contra la seguridad de la nación y el título segundo intitulado delitos contra el derecho internacional del libro segundo del Código Penal Federal, específicamente en los artículos 139 al 139 Ter y terrorismo internacional previsto en los artículos 148 Bis al 148 Quáter y que a continuación se agregan;

Artículo 139.- Se impondrá pena de prisión de quince a cuarenta años y cuatrocientos a mil doscientos días multa, sin perjuicio de las penas que correspondan por otros delitos que resulten:

I. A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos, o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, intencionalmente realice actos en contra de bienes o servicios, ya sea públicos o privados, o bien, en contra de la integridad física, emocional, o la vida de personas, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para atentar contra la seguridad nacional o presionar a la autoridad o a un particular, u obligar a éste para que tome una determinación.

II. Al que acuerde o prepare un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en territorio nacional.

Las sanciones a que se refiere el primer párrafo de este artículo se aumentarán en una mitad, cuando además:

I. El delito sea cometido en contra de un bien inmueble de acceso público;

II. Se genere un daño o perjuicio a la economía nacional, o

III. En la comisión del delito se detenga en calidad de rehén a una persona.

Artículo 139 Bis.- Se aplicará pena de uno a nueve años de prisión y de cien a trescientos días multa, a quien encubra a un terrorista, teniendo conocimiento de sus actividades o de su identidad.

Artículo 139 Ter.- Se aplicará pena de cinco a quince años de prisión y de doscientos a seiscientos días multa al que amenace con cometer el delito de terrorismo a que se refiere el párrafo primero del artículo 139.

Artículo 148 Bis.- Se impondrá pena de prisión de quince a cuarenta años y de cuatrocientos a mil doscientos días multa, sin perjuicio de las penas que correspondan por otros delitos que resulten:

I. A quien utilizando sustancias tóxicas, armas químicas, biológicas o similares, material radioactivo, material nuclear, combustible nuclear, mineral radiactivo, fuente de radiación o instrumentos que emitan radiaciones, explosivos o armas de fuego, o por incendio, inundación o por cualquier otro medio violento, realice en territorio mexicano, actos en contra de bienes, personas o servicios, de un Estado extranjero, o de cualquier organismo u organización internacionales, que produzcan alarma, temor o terror en la población o en un grupo o sector de ella, para presionar a la autoridad de ese Estado extranjero, u obligar a éste o a un organismo u organización internacionales para que tomen una determinación;

II. …;

III. …

IV. Al que acuerde o prepare en territorio mexicano un acto terrorista que se pretenda cometer, se esté cometiendo o se haya cometido en el extranjero.

…

Artículo 148 Ter.- Se impondrá pena de cinco a diez años de prisión y de cien a trescientos días multa, a quien encubra a un terrorista, teniendo conocimiento de su identidad o de que realiza alguna de las actividades previstas en el presente capítulo.

Artículo 148 Quáter.- Se aplicará pena de seis a doce años de prisión y de doscientos a seiscientos días multa al que amenace con cometer el delito de terrorismo a que se refieren las fracciones I a III del artículo 148 Bis.

Definitivamente la legislación mexicana carece de tipificación con respecto del ciberterrorismo; no hay manera de aplicar el tipo penal contemplado en el Código Penal Federal con respecto al terrorismo, toda vez que no menciona la utilización de la internet como medio de comisión, sólo establece la utilización de sustancias tóxicas, armas químicas, biológicas, instrumentos o materiales que emitan radiaciones, explosivos, armas de fuego, incendio, inundación u otro medio violento, aunque el fin es el mismo no el medio comisivo.

3.1.13. Grooming infantil

El grooming es una serie de conductas y acciones deliberadamente emprendidas por un adulto con el objetivo de ganarse la amistad de un menor de edad, creando una conexión emocional, con el fin de disminuir las inhibiciones del menor de edad y poder abusar sexualmente de él. En algunos casos, se puede buscar la inducción del menor al mundo de la prostitución infantil o la producción de material pornográfico.

El ciberacoso es una de las formas más comunes que puede sufrir un usuario de una red social, por la cual otras personas vulneran su dignidad, fama personal, reputación, estima.

Cuando en este tipo de actos se involucra un adulto que establece una relación "virtual" con un menor se denomina grooming. El adulto procede a tender lazos emocionales con el menor, obteniendo datos personales, luego en una tercera etapa provoca la desnudez del menor y, entonces, inicia el chantaje para seguir obteniendo material

obsceno a costa del menor.[66]

La preparación de Internet no difiere, pero el factor anonimato que trae las TIC permite que la persuasión progrese más rápido, ya que proporciona una manera sencilla en la que los adultos y los niños pueden tener discusiones sexualizadas. De hecho, el anonimato de las TIC significa que los adultos pueden asumir la personalidad de un niño disfrazando y luego hacer amistad a través de Internet con el niño víctima, creyendo que están en una relación con otro adolescente.

> *La investigación existente se centra en el alcance y la naturaleza de la pedofilia en línea y el abuso infantil, concentrándose abrumadoramente en el uso de ciertas tecnologías de Internet. Un ejemplo es el estudio de Bilstad (1996), que explora el uso de las tecnologías de tablero de noticias / boletines como una forma de publicar material obsceno.*
>
> *El estudio también incluye formas escritas de pornografía infantil. Del mismo modo, un estudio de Stanley (2002) cubre los perfiles psicológicos de los grupos de víctimas de riesgo y pedófilos y explora los métodos y tecnologías utilizados en la solicitud de los niños. Ambos estudios son útiles como guías sobre la naturaleza del problema, pero no proporcionan evidencia directa de cómo se manifiestan estos comportamientos, y no existen pruebas (experimentos) para teorías que exploren estrategias de grooming con niños "en riesgo".*[67]

Las leyes penales sobre el grooming infantil en línea representan una forma de penalización adicional de los actos del abuso fuera de línea de los niños. Dos instrumentos multilaterales, tanto de la región europea, como de la Convención sobre la Protección de la Infancia del Consejo de Europa (artículo 23) y de la Directiva de la UE sobre la Explotación Infantil[68] (artículo 6) establecen la penalización de tales actos. Los elementos centrales del delito incluyen la "propuesta intencional, a través de las tecnologías de la información y la

[66] Nava Garcés, Alberto E., *Delitos informáticos*, Tercera Edición, Editorial Porrúa, México, 2016, p.123

[67] K. Jaishankar, *Cyber Criminology, Exploring Internet Crimes and Criminal Behavior*, Taylor and Francis Group, LLC, Printed in the United States of America, 2011, p.81 “Newsgroups are discussion groups that utilize Usenet, a worldwide, non centralized group of services that stores messages and files and forwards their content to other servers on demand. Alt.Sex.Stories is one of many discussion groups within Usenet. Newsgroups are accessed through Newsgroup Readers software, which is designed to access Usenet”

[68] Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

comunicación"[69], por un adulto para conocer a un niño con el propósito de cometer un delito. Para que el delito sea cometido, ambos instrumentos también requieren actos materiales que conduzcan a tal reunión, por el perpetrador.

> *Convenio sobre la protección de la infancia del Consejo de Europa:*
>
> *Artículo 23. Proposiciones a niños con fines sexuales.*
>
> *Cada parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a del artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro.*
>
> *Directiva 2011/92/UE del Parlamento Europeo y del Consejo:*
>
> *Artículo 6.*
>
> *Embaucamiento de menores con fines sexuales por medios tecnológicos*
>
> *1. Los Estados miembros adoptarán las medidas necesarias para garantizar la punibilidad de las conductas dolosas siguientes:*
>
> *La propuesta por parte de un adulto, por medio de las tecnologías de la información y la comunicación, de encontrarse con un menor que no ha alcanzado la edad de consentimiento sexual, con el fin de cometer una infracción contemplada en el artículo 3, apartado 4, y en el artículo 5, apartado 6, cuando tal propuesta haya ido acompañada de actos materiales encaminados al encuentro, se castigará con penas privativas de libertad de una duración máxima de al menos un año.*
>
> *2. Los Estados miembros adoptarán las medidas necesarias para garantizar la punibilidad de cualquier tentativa de un adulto, por medio de las tecnologías de la información y la comunicación, de cometer las infracciones contempladas en el artículo 5, apartados 2 y 3, embaucando a un menor que no ha alcanzado la edad de consentimiento sexual para que le proporcione pornografía infantil en la que se represente a dicho menor.*

Con respecto de la legislación mexicana, no contempla el grooming infantil como delito informático, sin embargo, siendo rigurosos podría adecuarse, como es el mismo caso de la pornografía infantil, en la Ley General Para Prevenir, Sancionar y Erradicar los delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos delitos en su artículo 16, primer párrafo; que sí especifica entre otras conductas:

[69] Greenblatt, Sara, op. cit., nota 3, p. 103.

ARTÍCULO 16. Se impondrá pena de 15 a 30 años de prisión y de 2 mil a 60 mil días multa, así como el decomiso de los objetos, instrumentos y productos del delito, incluyendo la destrucción de los materiales resultantes, al que …

…induzca, por cualquier medio, a una persona menor de dieciocho años de edad, o que no tenga la capacidad de comprender el significado del hecho, o no tenga capacidad de resistir la conducta, a realizar actos sexuales…

3.2. Dogmática Jurídico Penal

La dogmática penal es el instrumento mediante el cual se facilita la interpretación progresiva del derecho vigente, en base al examen crítico, a la comparación y a la clasificación de la jurisprudencia, como puente entre la ley y la práctica. Desde esa vertiente, el llamado carácter tautológico de la dogmática jurídico-penal expresa lo que el Derecho dice y por qué lo dice. La dogmática posibilita la comprensión y sistematización del Derecho Positivo, permite, como única vía, la explicación del Derecho Penal en las universidades y la mejor aplicación en el campo jurisdiccional.[70]

La dogmática penal proyecta el soporte de tres tipos de investigaciones o procedimientos (Borja Jiménez): i) Investigación exegética, ii) Investigación sistemática y iii) Investigación crítica.

En este orden de ideas, la dogmática es el estudio exegético del texto de la ley realizando prácticamente una paráfrasis directa de su contenido, tomando casi textualmente lo que indica la ley sin margen para salirse de ésta; creando un proceso mediante el cual se relacionan los elementos del tipo penal para estructurar una adecuación exacta de las conductas a los diferentes prohibiciones en materia de delincuencia cibernética.

Se llama dogmática jurídica, precisamente porque los estudios que se realizan (por ejemplo: estudio dogmático del homicidio, lesiones, privación ilegal de la libertad, etc.,) parten de los dogmas contenidos en las leyes. Estos dogmas, fueron plasmados por el legislador; entonces, cuando el investigador realiza el estudio de esos dogmas para

[70] Nieves, Ricardo, *Teoría del Delito y Práctica penal, reflexiones dogmáticas y mirada crítica*. Escuela Nacional del Ministerio Público, Santo Domingo, República Dominicana, Editora Centenario, S. A.,2010, p.11

darles una sistematización coherente con la constitución y las leyes está realizando un estudio dogmático, y, en consecuencia, está haciendo ciencia del derecho.[71]

Nava Garcés sintetiza, en un arduo trabajo intelectual, el significado de la dogmática jurídico penal y nos regresa al camino correcto aclarando cual es el verdadero objeto de un análisis dogmático en las siguientes palabras:

> *En realidad, la dogmática jurídico penal es la disciplina que estudia el contenido de las normas jurídico penales para extraer su voluntad, con base en la interpretación, construcción y sistematización.*[72]
>
> *…A través de la sistematización lógica, científica de la dogmática penal, se garantiza a favor de los imputados un principio tan importante como lo es la legalidad, el apego irrestricto a la norma.*[73]

Por lo anterior, y haciendo un preámbulo al capítulo cuarto de este trabajo de tesis, vale la pena mencionar cual tan importante es el análisis técnico de la norma penal para las conductas tipificadas en el CPF concernientes a los cometidos a través de sistemas informáticos, en aras de salvaguardar esa garantía consagrada en el párrafo tercero del décimo cuarto constitucional.

3.3. Tipo Penal

En Alemania se han desarrollado los cuatro grandes sistemas de análisis de la teoría del delito que se emplean en todos aquellos países que, como México, tienen un sistema jurídico de tradición romano, canónica y germánica, a saber: clásico, neoclásico, finalista y funcionalista.[74] De lo anterior se desprende que el delito está constituido por una conducta y tres categorías como los denomina Díaz

---

[71] Jiménez Martínez, Javier, *la Teoría del Delito. Aproximación al estado de la discusión*. Editorial Porrúa. Primera edición. México 2010, p. 4

[72] Nava Garcés, Alberto Enrique, *Dogmática penal y teoría del delito, crítica y método*, 1a edición, Editorial Porrúa, México 2012, p.52

[73] ídem

[74] Díaz Aranda, Enrique, *Cuerpo del delito, probable responsabilidad y la reforma constitucional de 2008*, Instituto de Investigaciones Jurídicas, serie Estudios Jurídicos, Número 147. México, 2009, p.7

Aranda, estas son Tipicidad, Antijuridicidad y Culpabilidad. Para cuestiones del presente capítulo, nos concentraremos en el primero de estos elementos en todo lo que versa a la tipicidad, por ser ésta el juicio de adecuación de la conducta al tipo penal.

El tipo penal es la figura legislativa que nace con motivo del proceso de tipificación. Es la descripción abstracta de conducta que, a virtud del acto legislativo, queda plasmada o tipificada en la ley como garantía de libertad y seguridad, y como expresión técnica del alcance y contenido de la conducta injusta del hombre que se declara punible.[75] Por tanto, el tipo penal, se puede concebir como la descripción normativa que hace el legislador sobre la conducta prohibida y que la plasma en el código penal a través de su articulado.

En este tenor, Díaz Aranda citando a Ernst Beling, sugiere que el *tipo penal* se tradujo del vocablo alemán *tatbestand* que significa "supuesto de hecho"; y que en el sistema causalista o clásico, se caracterizó el *tipo* por ser objetivo y no valorativo, es decir, constituido por elementos objetivos o descriptivos; los elementos objetivos son todos aquellos que se perciben a través de los cinco sentidos y que son susceptibles de ser probados a través de la ciencia o pruebas científicas, lo que le llamó el tipo penal simple.

Sin embargo, dada su insuficiencia de elementos para explicar delitos como el robo donde se tiene que probar la ajenidad de la cosa, surgió el sistema neoclásico donde el tipo penal está constituido además de los elementos objetivos, de los normativos y subjetivos específicos cuando éste así se requiera; y donde los elementos normativos son conceptos de valoración jurídica o cultural, mientras que los elementos subjetivos específicos son los ánimos, fines, intenciones y propósitos de los sujetos.

[75] Cury Ursúa, Enrique, *Derecho Penal Parte General*, 2ª Edición, Editorial Jurídica de Chile, Tomo I, Santiago , Chile, 1992, p.278.

El sistema finalista de Welsel[76] aportó la inclusión del tipo subjetivo genérico compuesto por el dolo o la culpa; donde el dolo penal tiene siempre dos dimensiones, por un lado la voluntad tendiente a la realización típica y por otro como la conciencia del hecho y resolución al hecho, es decir el dolo es la voluntad de acción orientada a la realización del tipo de un delito; asimismo la culpa donde la voluntad de acción no se dirige al resultado típico realizado.

A decir de Orellana Wiarco[77], aparece en México en la década de los sesenta, una sistemática que apoya el método de la lógica formal simbólica del derecho penal, el cual se dio a la tarea de estudiar las sistemáticas causalista y finalista, no obstante el predominio de la legislación vigente por las concepciones de doctrinas extranjeras.

3.4. Bien jurídico

Para Díaz Aranda[78], la protección de bienes fundamentales para la sociedad es uno de los principios del derecho penal, en consecuencia las normas constitucionales permiten sostener del mandato que obliga al creador de la norma jurídica penal a expedir leyes, sí y sólo sí protegen esos bienes fundamentales; por tanto, la descripción del delito se justifica cuando las conductas lesionan o ponen en riesgo bienes jurídicos tutelados.

En este tenor, sólo se alcanzará la calidad de bien jurídico tutelado, aquello que el pueblo o la sociedad considera muy importante o imprescindible para su desarrollo social o individual, y éste es descrito en la ley penal como norma prohibitiva de conductas que los lesionan o ponen en riesgo, contemplando a la vez una consecuencia jurídica traducida en sanción penal.

> *Así se caracteriza el bien jurídico como "bien vital" reconocido socialmente como valioso como "valor jurídico" o "interés jurídico", como interés jurídicamente reconocido en un*

[76] Welzel, Hans, *Derecho Penal parte general*, traducción de Carlos Fontán Balestra, Editorial Roque Depalma, Buenos Aires, Argentina 1956.
[77] Orellana Wiarco, Octavio A., *Curso de derecho penal, Parte general*, Editorial Porrúa, Quinta edición corregida y aumentada. México, 2011.
[78] Díaz Aranda, Enrique y Roxin, Claus, *Teoría de la caso y del delito en el proceso penal acusatorio*, Straf, Primera edición, México 2015, p. 26.

determinado bien como tal en su manifestación general, como "la pretensión de respeto emanada de supuestos de hecho valiosos, en la medida en que los órganos estatales han de reaccionar con consecuencias jurídicas ante su lesión no permitida'", o como "unidad funcional valiosa". Y Kienapfel denomina bienes jurídicos a "valores, instituciones y estados jurídico penalmente protegidos, que son imprescindibles para la ordenada convivencia humana".[79]

Existen, por tanto, categorías axiológicas cuya valía ha sido reconocida históricamente como la vida, la integridad física, el patrimonio, la libertad, etcétera, y que además su importancia se refleja en la punibilidad descrita en el tipo penal. Por lo anterior, para la interpretación y aplicación del derecho penal será indispensable identificar el bien jurídico tutelado, su jerarquía y su correspondencia con la sanción.

3.5. Elementos del tipo penal

Siguiendo las ideas de Miguel Ángel Aguilar López[80], quien aborda en su estudio dogmático de los delitos, quien refiere que conforme al principio de legalidad, considera que los elementos del tipo penal son los contemplados por el numeral 168 del Código Procesal Federal posterior a la reforma del 1994 y que estuvo vigente hasta 1999, y a continuación se describen sus fracciones: I. La acción o la omisión, la lesión o puesta en peligro del bien jurídico tutelado; II. La forma de participación del sujeto activo; y III. El carácter doloso o culposo de la acción o la omisión; Incluso, si el tipo penal lo requiere se acreditarán: A)La calidad cualitativa y cuantitativa del activo y del pasivo; B) El objeto material; C)La atribuibilidad de la acción o la omisión al resultado; D)Los medios comisivos; E) Circunstancias de tiempo, modo, lugar y ocasión; F) Elementos normativos (culturales, jurídicos, doctrinarios y jurisprudenciales); G) Elementos subjetivos específicos (ánimos, deseos e intenciones); H) Los demás elementos que la ley prevé. Asimismo, resalta la importancia de que el legislador se esforzó para amalgamar las doctrinas modernas con el derecho positivo en aras de la seguridad jurídica, para que todo

[79] Roxin, Claus. *Derecho Penal parte general, tomo 1 fundamentos, La estructura de la teoría del delito*. Traducción de la 2a edición alemana, Editorial Civitas, Madrid España, 1997, p. 70
[80] Aguilar López, Miguel Ángel. *El delito y la responsabilidad penal, teoría, jurisprudencia y práctica*, Séptima edición, Editoral Porrúa, México, 2015, p. 150.

indiciado, imputado y sentenciado, estuviera en posibilidad de conocer la descripción del delito que se le imputa.

Señala Miguel Ángel que después de la reforma de 1999, se modificó para establecer ya no la acreditación de los elementos del tipo penal, sino del cuerpo del delito y la responsabilidad penal, sin embargo, señala, que a pesar de eso, los juzgadores continúan analizando en sus resoluciones, cada uno de los elementos de la descripción típica, evidenciando de esta forma la función garantista del poder judicial.

Ahora con la nueva normatividad adjetiva en materia penal, el estudio también se centra en específico sobre el numeral 405 de Código Nacional primera fracción:

Artículo 405. Sentencia absolutoria

En la sentencia absolutoria, el Tribunal de enjuiciamiento ordenará que se tome nota del levantamiento de las medidas cautelares, en todo índice o registro público y policial en el que figuren, y será ejecutable inmediatamente.

En su sentencia absolutoria el Tribunal de enjuiciamiento determinará la causa de exclusión del delito, para lo cual podrá tomar como referencia, en su caso, las causas de atipicidad, de justificación o inculpabilidad, bajo los rubros siguientes:

I. Son causas de atipicidad: la ausencia de voluntad o de conducta, la falta de alguno de los elementos del tipo penal, el consentimiento de la víctima que recaiga sobre algún bien jurídico disponible, el error de tipo vencible que recaiga sobre algún elemento del tipo penal que no admita, de acuerdo con el catálogo de delitos susceptibles de configurarse de forma culposa previsto en la legislación penal aplicable, así como el error de tipo invencible;

II. Son causas de justificación: el consentimiento presunto, la legítima defensa, el estado de necesidad justificante, el ejercicio de un derecho y el cumplimiento de un deber, o

III. Son causas de inculpabilidad: el error de prohibición invencible, el estado de necesidad disculpante, la inimputabilidad, y la inexigibilidad de otra conducta.

De ser el caso, el Tribunal de enjuiciamiento también podrá tomar como referencia que el error de prohibición vencible solamente atenúa la culpabilidad y con ello atenúa también la pena, dejando subsistente la presencia del dolo, igual como ocurre en los casos de exceso de legítima defensa e imputabilidad disminuida.

De esta forma, haciendo una descripción de la primera fracción a contrario sensu de este numeral, se tiene que hay tipicidad cuando exista voluntad en la conducta, se completen todos los elementos del tipo penal, cuando la víctima no haya dado su consentimiento sobre el bien jurídico tutelado disponible y que además no exista error de tipo vencible que recaiga sobre algún elemento del tipo penal que no admita la forma culposa.

De manera general, los elementos del tipo penal para la legislación mexicana está constituida en tres grupos los elementos objetivos, normativos y subjetivos; dentro del primer grupo está la descripción de la conducta, el objeto material, la atribuibilidad de la acción o la omisión al resultado o nexo causal, los medios comisivos; en el segundo grupo están las valoraciones que tiene que realizar el juzgador de expresiones de carácter normativo, cultural, doctrinal o jurisprudencial, que el mismo tipo penal contiene; finalmente el tercer grupo corresponde a la psique del sujeto activo, y que pueden ser los subjetivos genéricos dolo y culpa o los subjetivos específicos, concernientes a los ánimos, fines, propósitos que el legislador incluyó en el mismo tipo penal.

3.6. Dolo y Culpa

Como se desprende de la parte general del código sustantivo penal en su numeral séptimo, el delito es una conducta de acción por omisión y que será atribuible el resultado material tanto el que realice una conducta de acción como al que omita impedirlo, si éste último tenía el deber jurídico de evitarlo debido el deber de actuar es derivado de una ley que lo obligue, de un contrato que debía cumplir o de su propio actuar precedente al hecho.

A las acciones u omisiones de las que describe el párrafo anterior necesariamente se tienen que realizar de manera dolosa o culposa. Por lo que, obra con *dolo directo* quien, **conociendo** los elementos del tipo penal, **quiere** el resultado típico del hecho descrito por la ley; asimismo, que obra con *dolo eventual* quien **previendo** como posible el resultado típico, **acepta** la realización del hecho descrito por la ley.

En este tenor, obra con *culpa sin representación* quien produce el resultado típico, **no previendo** siendo **previsible** u obra con *culpa con representación* quien produce el resultado típico **previendo** pero **confiando** en que no se produciría, todo en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales.

Me parece importante recordar las tres modalidades del delito, es *instantáneo*, cuando la consumación se agota en el mismo momento en que se han realizado todos los elementos de la descripción penal; es *permanente o continuo*, cuando la consumación se prolonga en el tiempo, y es *continuado*, cuando con unidad de propósito delictivo, pluralidad de conductas y unidad de sujeto pasivo, se viola el mismo precepto legal.

Finalmente a manera de resumen del tercer capítulo, se han desarrollado groso modo los delitos más significativos que se cometen a través de medios electrónicos de comunicación y que en sede internacional se han documentado para hacer extensiva su regulación legislativa interna, sobre todo para las naciones parte del Convenio de Budapest contra la ciberdelincuencia, de tal suerte que exista una coordinación global en su combate y control. Así mismo, se revisó de forma por demás compacta las bases técnicas de la dogmática penal y los elementos del tipo penal, para efecto de utilizarlos en el siguiente capítulo donde se desarrolla una propuesta para un análisis técnico de los elementos de cada tipo penal relacionados con los sistemas informáticos y que están contenidos en el CPF.

CAPÍTULO CUARTO

ASPECTOS TÉCNICOS DE LOS ELEMENTOS DEL TIPO PENAL PARA LOS DELITOS INFORMÁTICOS DEL CODIGO PENAL FEDERAL

Una vez que hemos definido en qué consisten los delitos informáticos, así como las diferentes legislaciones que los tipifican, tanto en sede local como internacional, procedo a realizar el siguiente capítulo concerniente al enfoque dogmático, teórico, sistemático de los tipos penales para los delitos informáticos, el cual implica analizar sus elementos y requisitos, a partir de diversos contenidos de la ley penal, tanto generales como particulares, porque todos y cada uno de ellos constituye un presupuesto para realizar el ejercicio de la punición. Por ende, esos elementos se derivan de los contenidos, tanto la parte general como la especial de la ley, por ser ésta la única fuente del derecho penal.

Es menester para el que suscribe, la realización de un estudio técnico del tipo penal toda vez que a la luz del principio de tipicidad, como pilar que sustenta al de legalidad en materia penal consagrado en el párrafo tercero del artículo 14 de la CPEUM en su última reforma publicada DOF 24-02-2017; y el cual, es una exigencia normativa clara y precisa de las conductas ilícitas. Es decir, la descripción que hace el legislador de las conductas ilícitas debe contener la información necesaria para realizar el proceso mental de adecuación típica, sin necesidad de recurrir a complementaciones legales más allá de su interpretación, para no caer en terreno de la analogía.

El estudio técnico del tipo penal de *Acceso ilícito a sistemas y equipos de informática*, contenido en el capítulo II del Título Noveno en el Código Penal Federal y que a través de sus numerales 211 Bis 1, 211 Bis 2, 211 Bis 3, 211 Bis 4 y 211 Bis 5, desarrollan las conductas típicas que con relación a la informática contiene la normatividad federal en México. A continuación procedo al desarrollo

interpretativo del contenido de tipo penal para cada uno de los artículos mencionados.

4.1. Artículo 211 BIS 1

PARA EL ARTÍCULO 211 BIS 1, DENTRO DEL CUAL SE CONTIENE LA HIPÓTESIS NORMATIVA DESCRIBIENDO LO SIGUIENTE:

> *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.*

A) Con respecto a la hipótesis de modificar la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, ésta se acreditará con los elementos siguientes:

ELEMENTOS OBJETIVOS

Como elementos objetivos o externos que constituyen la materialidad del hecho que la ley señala como delito, la acreditación de la acción fáctica de modificar cualquier información ya sea escrita, gráfica, en video, en voz, archivos, programas, software, contenida en cualquier unidad de almacenamiento dentro del sistema o equipo de informática como disco duro, memoria ROM, memoria RAM, Flash Card, disquete, CD-RW, unidad USB o unidad SD.

Con esta conducta de acción se vulnera el bien jurídico tutelado que la sociedad emergente de la Información hace con la incorporación de valores inmateriales y de la información misma, como bienes jurídicos de protección, esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible; esto por cuanto la información no puede, a criterio de Alejandro Rojas,[81] ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que esa información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida; y por lo que respecta a la Convención de Budapest contra la ciberdelincuencia se menoscaba la *confidencialidad*, la *integridad* y la *disponibilidad* de los datos y sistemas informáticos.

> *En todas las legislaciones del universo se le da un nombre diverso a las conductas ilegales ejecutadas por los ciberdelincuentes, en lo que atañe a lo que se conoce como delitos informáticos, y en Colombia, mediante la ley doce setenta y tres del cinco de enero de dos mil nueve se creó un nuevo bien jurídico tutelado y el codificador lo denominó "De la protección de la información y de los datos"*
>
> *Las acciones de la cibercriminalidad producen un doble quebrantamiento; de un lado el interés económico o patrimonial de las personas y la de un interés estatal por la protección, defensa y salvaguardia del buen funcionamiento de los sistemas informáticos, valga decir, de la información y de los datos.*[82]

Otro elemento objetivo se relaciona con la calidad del sujeto activo, el artículo señala claramente que es cualquier persona que no tenga autorización, se entiende que la autorización deviene del propietario del sistema o equipo de informática; esto es, en el contexto de la ingeniería de seguridad informática, la autorización es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello. Los recursos incluyen archivos y otros

[81] Virumbrales de Rojas, Alejandro, *Regulación penal de la delincuencia informática*, Universidad de Valladolid, Julio 2015 https://uvadoc.uva.es/bitstream/10324/13740/1/TFG-D_0124.pdf, Consulta 24 de julio 2107, 23:50

[82] Palomá Parra, Luis Orlando, op. cit. nota 21, p.64.

objetos de datos, programas, dispositivos y funcionalidades provistas por aplicaciones.

> *Sujeto activo, llámese así al agente del delito, quien mediante una conducta, sea ésta de carácter positivo o negativo, realiza un hecho tipificado en la ley como delito. La ley no establece una cualidad específica para el sujeto activo; sin embargo, se entiende que estos delincuentes poseen habilidades específicas para el manejo de sistemas informáticos. Esto no es, claro está, un requisito indispensable.*[83]

El objeto material, como elemento objetivo de este ilícito lo constituye el objeto modificado, en este caso es la información; para cuestiones de reparación del daño ocasionado por la comisión de la conducta de acción implica la restitución del objeto material y, si no fuese posible, el pago de su valor actualizado; sin embargo, cuando no sea factible su restitución y en la causa no obre una identificación clara e integral del objeto material modificado, que permita establecer su valor, es incorrecto que el juzgador condene al sentenciado a entregar a la víctima u ofendido una cosa "semejante" o "distinta" a la que fue materia de la modificación, porque ello viola el derecho de seguridad jurídica del sentenciado, al no existir un parámetro que dé certeza para cumplir esa sentencia.

López Betancourt señala que *el objeto material en el delito de Acceso ilícito a sistemas y equipos de informática, consiste en la información que se pretende resguardar, contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, sean de particulares, instituciones financieras o del Estado.*[84]

El tipo penal no requiere el medio específico para la consumación del hecho, esto es, el medio comisivo; puede ser el acceso en la misma computadora o bien a través de la red local o internet. Sin embargo, hay autores que refieren como medios comisivos las aplicaciones con que se vale el sujeto activo para penetrar al sistema informático.

---

[83] López Betancourt, Eduardo, *Delitos en particular 4*, Tercera edición, Editorial Porrúa México, 2016, p.304
[84] Ibídem, p.305

> *Algunos de los medios para desplegar la conducta, particularmente en el uso de códigos maliciosos, los cuales son programas de cómputo diseñados para hacer que los equipos de cómputo (móviles y fijos) realicen procesos o acciones distintas a las que fueron programados originalmente sin el consentimiento del usuario cuyos objetivos son: ataque a sistemas de archivos, sistemas operativos, de procesamiento, de comunicación, de almacenamiento, a extensiones de archivos o aplicaciones específicas.*[85]

En cuanto a las circunstancias de tiempo, modo y ocasión, el tipo sólo se especifica la ocasión en el momento en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, entendido éste como un antivirus, clave de acceso por contraseña o un firewall.

ELEMENTOS NORMATIVOS

Para los elementos normativos; se tienen las siguientes expresiones semánticas: *autorización*, *información*, *sistemas o equipo de informática* y *modificar*.

Donde, la expresión *autorización* se desprende de una interpretación doctrinal y que a decir de Rafael De Pina[86], es un acto de naturaleza judicial, administrativa o, simplemente privado, en virtud del cual una persona queda facultada para ejercer determinado cargo o función o para realizar determinado acto de la vida civil.

Mientras que la expresión semántica *información* puede provenir de un aspecto cultural, no obstante la misma CPEUM en su última reforma publicada DOF 24-02-2017, hace énfasis sobre la misma al referir que toda persona tiene derecho a la protección de sus datos personales, sin aludir su materialidad, por lo que un sistema de cómputo puede contener, como ya se expresó con anterioridad, información almacenada de identificación (nombre, domicilio, teléfono, correo

[85] Montoya Piña, Javier Omar, *Delitos federales cometidos a través de medios informáticos*, Editorial Flores Editor y Distribuidor, SA de CV., México, 2015, p.93
[86] De Pina Vara, Rafael, *Diccionario de Derecho*, 37ª Edición, segunda reimpresión, Editorial Porrúa, México 2012, p. 117.

electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etc.); laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); patrimoniales (información fiscal, historial crediticio, etc.); y que en este contexto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la define como: datos personales son cualquier información concerniente a una persona física identificada o identificable; la cual desde el punto de vista de su formato, el concepto de datos personales abarca la información en cualquier modo, sea alfabética, numérica, gráfica, fotográfica o sonora, por citar algunas, y puede estar contenida en cualquier soporte como en papel, en la memoria de un equipo informático, en una cinta de video o en un dvd.

Por otro lado, con respecto de la expresión *sistema o equipo informático,* se relaciona a los instrumentos creados por el ser humano como herramienta con diferentes usos; desde los educativos, de comunicación, de trabajo, hasta los de entretenimiento, entre otros; Además, el equipo de cómputo puede estar formado por los siguientes elementos: i) C.P.U (Unidad Central de Proceso), ii) Monitor, iii) Teclado, iv) Mouse, v) Impresora; los cuales son los que hacen funcionar a un equipo de cómputo y cabe mencionar que cada uno de ellos tiene una función específica que optimizara las etapas de su operatividad, tales como la entrada, el procesamiento y la salida.

> *Los computadores, arquitectura externa (hardware), un procesador o unidad central de proceso, se encarga de procesar las instrucciones y los datos. La memoria RAM, los chips en los que el procesador almacena de forma temporal los datos y los programas. Disco duro, es el dispositivo de almacenamiento permanente interno en el que se guardan todos los programas y archivos, su capacidad se mide en gigabytes (GB).*
>
> *La unidad de CD-ROM, sirve para leer los discos compactos en los que vienen casi todos los programas. Unidad de de CD RW, permite en un disco compacto, escribir y guardar información con capacidades de 650 megabytes 8MG). Tarjeta madre, aloja los principales componentes del computador, como el procesador, la memoria RAM, las ranuras de expansión, etc. Puertos USB (Universal Serial Bus) que facilita la conexión de periféricos externos como el monitor, el mouse, el teclado, impresoras; el puerto USB permite transferir datos a 12 Mbps.*[87]

[87] Díaz García, Alexander, *Derecho Informático, elementos de la informática jurídica*, 1a reimpresión, Editorial Leyer, Colombia, 2012. p.27

En tanto que el verbo rector *modificar*, es hacer una cosa diferente de como era antes, alterar, enmendar, reformar o transformar una cosa alterando sus características.

ELEMENTOS SUBJETIVOS

El elemento subjetivo genérico dolo, se actualiza en su modalidad de dolo directo toda vez que este tipo de delitos el sujeto activo, conoce los elementos del tipo penal al ingresar a un sistema o equipo informático sin autorización, es decir no es casual o por error su ingreso pues quiere el resultado típico del hecho descrito por la ley, toda vez que para realizar la conducta se es conocedor de que está prohibida por una norma jurídica, no obstante quiere su realización al ratificar y aceptar en el momento mismo de que el sistema de cómputo cuestiona sobre la intención de modificar esa información con las ventanas de diálogo que aparecen en el sistema operativo.

> *Durante la fase interna, el sujeto decide realizar el delito de Acceso ilícito a sistemas y equipos de informática, concibiendo, deliberando y decidiendo conscientemente realizar el acto; En la fase externa, el agente hace externo su deseo de cometer un crimen, realizando las acciones preparatorias para cometer el ilícito, y finalmente lo lleva a cabo.*[88]

B) Con respecto a la modalidad de destruir la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, ésta se acreditará con los elementos siguientes:

ELEMENTOS OBJETIVOS

Los elementos objetivos, primeramente lo constituyen, entre otros, la materialidad de la conducta tipificada en la ley penal con la acreditación de la acción fáctica

[88] López Betancourt, Eduardo, op. cit. nota 83, p.311.

voluntaria de destruir la información contenida en cualquier unidad de almacenamiento del sistema o equipo de cómputo, en cualquiera de sus diferentes formatos, ya sea en archivo, video, audio o gráfica.

Mediante esta conducta de acción también se lesiona el bien jurídico tutelado que la sociedad ha incorporado como valores inmateriales y de la información misma, jurídicamente tutelados, considerando las diferencias existentes por ejemplo entre la propiedad tangible y la intangible; y por lo que respecta a la Convención de Budapest contra la ciberdelincuencia se menoscaba la *confidencialidad*, la *integridad* y la *disponibilidad* de los datos y sistemas informáticos, esto por cuanto la información no puede ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien es cierto que dichos bienes tienen un valor intrínseco compartido como valoración económica, también lo es que esa información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida, como es el caso de los datos personales.

En consecuencia, porque así lo requiere el tipo penal, la calidad del sujeto activo debe ser cualquier persona que no tenga autorización, y como ya se dijo, se entiende que la autorización deviene del propietario y que en el contexto de la ingeniería de seguridad informática, la autorización es una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello; los recursos incluyen archivos y otros objetos de datos, programas, dispositivos y funcionalidad prevista por aplicaciones.

> *El objeto material es la persona o cosa (todo lo que tiene entidad, ya sea corporal o espiritual, natural o artificial, real o abstracta) sobre la que recae directamente el delito o el daño causado por el delito cometido. Lo pueden ser cualquiera de los sujetos pasivos, las cosas animadas o inanimadas y ahora, las virtuales.*[89]

[89] Nava Garcés, Alberto E., op. cit. nota 66, p.87

El objeto material está constituido por la información contenida en las unidades de almacenamiento del sistema o equipo de cómputo; para cuestiones de reparación del daño ocasionado por la comisión de la conducta de destrucción, lo que implica la imposibilidad de recuperación, por lo que el pago de su valor actualizado, y en la causa no obre una identificación clara e integral del objeto material destruido, que permita establecer su valor, es incorrecto que el juzgador condene al sentenciado a entregar a la víctima u ofendido una cosa "semejante" o "distinta" a la que fue materia de la destrucción, porque también violaría la garantía de seguridad jurídica del sentenciado, al no existir un parámetro que dé certeza para cumplir esa sentencia.

Con respecto de los medios comisivos, el tipo penal no requiere el medio específico para la consumación del hecho, esto es, que para la destrucción de la información contenida en un sistema o equipo de cómputo puede ser el acceso en el mismo sistema, en la misma computadora o bien a través de la red local o de internet.

Con relación de las circunstancias de tiempo, modo, lugar y ocasión, sólo refiere el tipo penal que se actualiza el supuesto, en el momento en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, entendido este como un antivirus, una clave de acceso por contraseña o un firewall; no obstante, la seguridad informática se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable; en un ambiente de red, un mecanismo de seguridad es la habilidad de identificar y eliminar vulnerabilidades, consecuentemente si, el administrador del sistema o bien el propietario no actualiza un sistema de seguridad informática y éste es vulnerado por cualquier persona habría adecuación de la conducta al tipo.

ELEMENTOS NORMATIVOS

Para los elementos normativos, se presentan cuatro expresiones semánticas a saber: *autorización*, *información*, *sistemas u equipo de informática* y *destruir*.

Donde la *autorización*, derivada de una interpretación doctrinal, es un acto de naturaleza judicial, administrativa o, simplemente privado, en virtud del cual una persona queda facultada para ejercer determinado cargo o función o para realizar determinado acto de la vida civil.

Mientras que la *información* puede provenir de un aspecto cultural y legal en estricto sensu, pues se encuentra inmersa en la misma CPEUM en su última reforma publicada DOF 24-02-2017, cuando enfatiza que toda persona tiene derecho a la protección de sus datos personales, sin aludir a su materialidad, por lo que un sistema de cómputo puede contener, como ya se expreso con anterioridad, información almacenada de la identificación de sus propietarios como el nombre, el domicilio, el número telefónico, su correo electrónico, la firma, RFC, CURP, la fecha de nacimiento, la edad, la nacionalidad, el estado civil, etcétera; asimismo información laboral (puesto, domicilio, correo electrónico y teléfono del trabajo); además de patrimoniales (información fiscal, historial crediticio, etc.); y que en este contexto también la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, define a los datos personales como cualquier información concerniente a una persona física identificada o identificable; a la vez la Ley de Firma Electrónica Avanzada, define a un documento electrónico como aquél que es generado, consultado, modificado o procesado por medios electrónicos; y en el aspecto cultural, la información personal, está expresada en cualquier modo, sea alfabética, numérica, gráfica, fotográfica o sonora, por citar algunas formas, y puede estar contenida en cualquier soporte como en papel, en la memoria de un equipo informático, en una cinta de video o en un dvd.

Así las cosas, con respecto de la expresión *sistema o equipo de cómputo,* se relaciona con los instrumentos creados por el ser humano como herramienta, con diferentes usos desde educativos, de comunicación, de trabajo, de

entretenimiento, etcétera; además, el equipo de cómputo está formado por los siguientes elementos: i) C.P.U (Unidad Central de Proceso), ii) Monitor, iii) Teclado, iv) Mouse, v) Impresora; los cuales funcionan de manera armónica, desempeñando una función específica en el sistema.

Finalmente, y con respecto al verbo rector *destruir*, el cual es un término meramente doctrinal y que el diccionario de la real academia española lo define como reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño, deshacer o inutilizar algo; por lo que para cuestiones de reparación del daño se ve impedida en virtud de que este ilícito origina un detrimento en el patrimonio y en atención a que el valor consignado en la misma información es lo que permite punir la conducta del activo.

ELEMENTOS SUBJETIVOS

El elemento subjetivo genérico con carácter doloso de la conducta en su modalidad de dolo directo, toda vez que en este tipo de delitos el sujeto activo cumple con el elemento cognoscitivo, al conocer de los elementos del tipo penal, además del elemento volitivo cuando quiere el resultado típico del hecho descrito por la ley, el cual es la destrucción de la información; estos elementos se ratifican de manera fáctica cuando el sistema o equipo de cómputo cuestiona sobre la destrucción de la información y sobre todo por tratarse de daños en propiedad ajena.

> *En este tipo penal se podría analizar por voluntad dolosa todas aquellas acciones y mecanismos de interferir sistemas de información mediante el despliegue de operaciones con conocimientos avanzados en el tema. Este delito presupone una conducta dolosa, toda vez que el agente o sujeto activo cuenta con los conocimientos necesarios para poder manipular la información de cualquier ordenador y tiene toda la intención para hacerlo.*
>
> *El sujeto continúa dolosamente, es decir, comprende el sentido formal de los elementos esenciales del tipo penal y quiere la realización de dichos elementos, quiere la acción delictiva, en este caso modificar, destruir o provocar pérdida de información.*[90]

[90] Montoya Piña, Javier Omar, op. cit. nota 86, p.95

C) Con respecto a la modalidad de causar la pérdida de la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, ésta se acreditará con los elementos siguientes:

ELEMENTOS OBJETIVOS

Primeramente con la realización material del activo de todos los actos idóneos de ejecución para que de manera voluntaria y mediante una conducta de acción cause la pérdida, ya sea de manera parcial o total de la información contenida en cualquier dispositivo de almacenamiento perteneciente al sistema o equipo de informática, y en cualquiera de sus diferentes formatos, en archivo, video, audio o gráfica.

Con esta conducta de acción se lesiona los bienes jurídicos tutelados que la legislación penal mexicana establece en valores *inmateriales* y de la *información* misma; además con relación de la Convención de Budapest contra la ciberdelincuencia, de la que Estado mexicano es parte desde 2014, se menoscaba la *confidencialidad*, la *integridad* y la *disponibilidad* de los datos y sistemas informáticos.

Porque así lo requiere el tipo penal, la calidad del sujeto activo, debe ser cualquier persona que no tenga autorización, se entiende que la autorización deviene del propietario del equipo informático o de la persona encargada llamado administrador del sistema informático y que en materia de ingeniería de seguridad informática, la autorización es también una parte del sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello; los recursos incluyen archivos y otros objetos de datos, programas, dispositivos y funcionalidad prevista por aplicaciones.

> *En este rubro cabe hacer mención que si bien es cierto el tipo penal no requiere una calidad específica, no obstante el sujeto activo presenta ciertas características que lo distinguen del común de los delincuentes, esto es, tiene habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos en donde se maneja información de carácter relevante, o bien cuenta con los conocimientos teóricos y prácticos respecto del uso de los sistemas informatizados.*[91]

El objeto material sobre el que recae la conducta lesiva está constituido por la información contenida en los elementos estructurales encargados de resguardar los datos dentro del sistema o equipo informático; para cuestiones de reparación del daño ocasionado por la comisión de la conducta de causar la pérdida de información, no es posible su reparación ni su restitución, por lo que devendría el pago de su valor actualizado, claro y preciso en dinero, sin que se permita entregar a la víctima u ofendido una cosa "semejante" o "distinta" a la que fue materia de la pérdida, en aras de la garantía de seguridad jurídica del sentenciado, al existir un parámetro que dé certeza para cumplir ese mandato resarcitorio.

En cuanto a los medios comisivos, el tipo penal no requiere el medio específico para la consumación del hecho, esto es, que para causar la pérdida de la información contenida en un sistema o equipo informático, ésta puede ser de cualquier manera, es decir, accediendo al sistema localmente, vía remota, con la utilización de virus informáticos enviados a manera de SPAM o bien, con la destrucción material del hardware que constituye el equipo informático.

Referente a la circunstancias de tiempo, modo, lugar y ocasión, el ilícito se actualizará en la ocasión misma en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, entendida como seguridad informática la que se ocupan de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable; en un ambiente de red, un mecanismo de seguridad es la habilidad de identificar y eliminar vulnerabilidades; por ende, este mecanismo de seguridad es un requisito

[91] Ibídem, p.101

del tipo penal para que se actualice, en un momento dado, la conducta ilícita de causar la pérdida de información electrónica.

ELEMENTOS NORMATIVOS

Siguiendo con los elementos normativos del tipo penal, se concurren cuatro expresiones: *autorización*, *información*, *sistemas u equipo de informática* y *causar la pérdida.*

Haciendo una descripción de cada uno se tiene que con relación a la *autorización*, ésta derivada de una interpretación doctrinal, y que dentro del contexto de la informática es aquel usuario autorizado[92], en materia de telecomunicaciones se define, como aquella persona física o moral, que en forma eventual o permanente tiene acceso a algún servicio público o privado de telecomunicaciones.

Mientras que la *información* puede provenir de un aspecto doctrinal y legal en estricto sensu, toda vez que la misma Convención sobre la Ciberdelincuencia define de manera expresa que por datos informáticos se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función; asimismo la Ley de Firma Electrónica Avanzada publicada en el Diario Oficial de la Federación el 11 de enero de 2012, define a un documento electrónico como aquél que es generado, consultado, modificado o procesado por medios electrónicos; además, en el aspecto doctrinal, los datos informáticos se les define como el conjunto de hechos o condiciones que pueden ser objeto de una comunicación, de una interpretación o de un tratamiento personal,[93] y que está expresada en forma, alfabética, numérica, gráfica, fotográfica o sonora, por citar algunas.

[92] Cienfuegos Salgado, David y Vázquez Mellado, Julio Cesar, *Vocabulario Judicial,* Instituto de la Judicatura Federal – Escuela Judicial. Primera edición, México, 2014, p.536.
[93] Rodríguez Aragón, Licencio, *Información e Informática, Informática Básica*, Departamento de Informática, Estadística y Telemática, Universidad de Castilla La Mancha, España,

Por otro lado, con respecto de la expresión *sistema o equipo de cómputo,* conforme al Convenio de Budapest,[94] por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

Finalmente, con respecto del verbo rector *causar la pérdida*, se desprende de una interpretación doctrinal y se entiende como producir cierto efecto o al dar lugar a cierta consecuencia, que para el caso, es la pérdida irreparable de la información o datos contenidos dentro del sistema o equipo informático.

ELEMENTOS SUBJETIVOS

El elemento subjetivo genérico consistente en el dolo en su modalidad de dolo directo, de tal suerte que se presentan en la psique del sujeto activo, tanto el elemento cognoscitivo al conocer de los elementos del tipo penal, como el elemento volitivo al querer el resultado típico de causar la pérdida de la información ya sea en sistemas o en equipos de informática, el cual es la destrucción de la información, la acreditación de este elemento debe estar relacionada con indicios consistentes en que de un hecho conocido, se induce otro desconocido, mediante un argumento probatorio obtenido de aquél, en virtud de una operación lógica crítica basada en normas generales de la experiencia o en principios científicos o técnicos, que en este caso es presumir que para lograr acceder a la información contenida en el equipo informático, debió primeramente encender otro equipo informático, conectarse a una red de servicio de internet, si fuera el caso, luego acceder mediante un proceso de conexión remota a la terminal destino, una vez dentro, buscar dentro de las unidades de almacenamiento específicas y causar la pérdida de la información, luego

---

https://previa.uclm.es/profesorado/licesio/Docencia/IB/IBTema1.pdf; consulta 25 de julio de 2017, 20:31

[94] Convenio sobre la Ciberdelincuencia, Budapest, 23.X1.2001, http://www.oas.org/juridico/english/cyb_ pry_convenio.pdf. Consulta 25 de julio de 2017, 21:00.

entonces, todos estos pasos concatenados de manera secuencial nos demuestran que su actuar no fue circunstancial o imprudencial, sino que actuó con conocimiento firme de querer el resultado material del hecho.

D) Con relación al segundo párrafo del tipo penal en cuestión, se encuentran dos hipótesis la de conocer y luego la de copiar la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, éstas se actualizarán con la acreditación de los siguientes elementos:

ELEMENTOS OBJETIVOS

En lo concerniente a los elementos objetivos perceptibles a través de los sentidos, donde primeramente con la acreditación de un comportamiento a manera de acción concretizada para conocer el contenido de un sistema o equipo informático, al estar ese contenido representado como información o datos almacenados en cualquiera de los dispositivo destinados para tal fin y que esté integrado al sistema informático, en forma de memoria interna o unidades móviles como USB o SD.

En segundo término, con la acreditación de la conducta por parte del sujeto activo en forma de acción consumada para copiar cualquier información, ya sea en archivo electrónico, por gráficas, en video, en voz, programas, software; la cual es extraída de cualquier unidad de almacenamiento dentro del sistema o equipo de informática como disco duro, memoria, Flash Card, disquete, CD-RW, USB o SD.

Con cualquiera de estas dos conductas descritas como acción de conocer o copiar, se vulnera el bien jurídico tutelado de la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que la Convención de Budapest sobre ciberdelincuencia ha definido, desde su creación en Noviembre de 2001, y que el Estado Mexicano como parte de la misma desde el 2014 está obligado a respetar, proteger y garantizar.

Siguiendo con los elementos objetivos, y con respecto de la calidad del sujeto activo, el numeral 211 Bis 1 en su segundo párrafo es claro al establecer que trasgrede la norma jurídica al que sin autorización, donde por su carácter cualitativo la autorización; se entiende desde una interpretación doctrinal el permiso otorgado por el propietario del sistema o equipo informático, expresado a través del mismo sistema operativo que protege los recursos del sistema permitiendo que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello; los recursos incluyen archivos, datos, programas, dispositivos, hardware y funcionalidades provistas por aplicaciones.

Con relación al objeto material, en el que recaen directamente las lesiones señaladas como conocer o copiar, lo constituye el conjunto de datos que de manera electrónica conforman la información contenida en las unidades de almacenamiento del sistema o equipo informático; y que para reparar el daño ocasionado en lo concerniente al conocimiento de la información no implicaría la restitución del objeto material toda vez que por ser un tipo de resultado formal no hay sustracción del mismo; en cuanto a la conducta lesiva de copiar los datos informáticos sí implicaría la restitución o devolución del objeto material y si no fuese posible, el pago de su valor actualizado y precisado en dinero.

El tipo penal no requiere el medio específico para la consumación del hecho, esto es, el medio comisivo puede ser el acceso a través de la misma computadora o bien a través de la red local o internet.

En cuanto a las circunstancias de tiempo, modo, lugar y ocasión, al considerar ésta última, el tipo sólo especifica el momento mismo en que el sistema o equipo informático se encuentre protegido por algún mecanismo de seguridad, como puede ser antivirus, clave de acceso por contraseña, firewall, filtros de tráfico de red, reglas de filtrado de patrones, políticas permisivas o restrictivas, un Sistema de Detección de Intrusos o IDS (Intrusion Detection System), etcétera.

ELEMENTOS NORMATIVOS

Pasando a los elementos normativos, representados por las expresiones semánticas *autorización*, *información*, *sistemas u equipo de informática*, *conocer* y *copiar.*

Donde la autorización, se desprende de una interpretación doctrinal y que a decir de Rafael De Pina, es un acto de naturaleza judicial, administrativa o, simplemente privado, en virtud del cual una persona queda facultada para ejercer determinado cargo o función o para realizar determinado acto de la vida civil.

En tanto que la expresión *información* tiene dos vertientes de interpretación, una cultural, y otra legal toda vez que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la define como: datos personales, lo constituye cualquier información concerniente a una persona física identificada o identificable; asimismo, la Convención de Budapest sobre la ciberdelincuencia entiende por datos informáticos, cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función; y culturalmente la información es el conjunto de datos electrónicos almacenada dentro de los sistemas informáticos en forma, alfabética, numérica, gráfica, fotográfica, visual o sonora, por citar algunas, y que puede estar contenida en cualquier tipo de unidad de almacenamiento como la memoria de un equipo informático, en una cinta de video o en un dvd.

Para la expresión *sistema o equipo de cómputo*, la misma Convención de Budapest entiende por “sistema informático, todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

Con respecto del los verbos rectores de las conductas de *conocer* y *copiar*; *conocer* es , según el diccionario de la real academia española, entender, advertir, saber, percibir, averiguar por el ejercicio de las facultades intelectuales la

naturaleza, cualidades y relaciones de las cosas; mientras que *copiar*, es reproducir una obra exactamente igual, o muy parecida, que otra.

ELEMENTOS SUBJETIVOS

El elemento subjetivo genérico dolo, igual que los análisis anteriores, se configura en su modalidad de dolo directo toda vez que en términos del artículo noveno del Código Federal penal, este tipo de delitos el sujeto activo, conoce los elementos del tipo penal, y quiere el resultado típico del hecho, toda vez que para realizar la conducta se es conocedor de que está prohibida por una norma jurídica, no obstante quiere su realización, por un lado de conocer la información contenida en el sistema o equipo informático, toda vez que, al estar éste protegido con el sistema de seguridad logra el acceso para imponerse al conocimiento, y por otro lado quiere la conducta ilícita al proceder con la trasferencia de la información almacenada en el sistema o equipo informático para ser copiada a otra unidad de almacenamiento de su propiedad; la manera de acreditar el dolo en esta conducta, puede comprobarse con la prueba circunstancial o de indicios, la cual consiste en que de un hecho conocido, se induce otro desconocido, mediante un argumento probatorio obtenido de aquél, en virtud de una operación lógica crítica basada en normas generales de la experiencia o en principios científicos o técnicos, como se desprende de la siguiente tesis de la primera sala:

> *Época: Novena Época; Registro: 175606; Instancia: Primera Sala; Tipo de Tesis: Aislada; Fuente: Semanario Judicial de la Federación y su Gaceta; Tomo XXIII, Marzo de 2006; Materia(s): Penal; Tesis: 1a. CVII/2005; Página: 205*
>
> *DOLO DIRECTO. SU ACREDITACIÓN MEDIANTE LA PRUEBA CIRCUNSTANCIAL.*
>
> *El dolo directo se presenta cuando el sujeto activo, mediante su conducta, quiere provocar directamente o prevé como seguro, el resultado típico de un delito. Así, la comprobación del dolo requiere necesariamente la acreditación de que el sujeto activo tiene conocimiento de los elementos objetivos y normativos del tipo penal y quiere la realización del hecho descrito por la ley. Por ello, al ser el dolo un elemento subjetivo que atañe a la psique del individuo, la prueba idónea para acreditarlo es la confesión del agente del delito. Empero, ante su ausencia, puede comprobarse con la prueba circunstancial o de indicios, la cual consiste en que de un hecho conocido, se induce otro desconocido, mediante un argumento probatorio obtenido de aquél, en virtud de una operación lógica crítica basada en normas generales de la experiencia o en principios*

científicos o técnicos. En efecto, para la valoración de las pruebas, el juzgador goza de libertad para emplear todos los medios de investigación no reprobados por la ley, a fin de demostrar los elementos del delito -entre ellos el dolo-, por lo que puede apreciar en conciencia el valor de los indicios hasta poder considerarlos como prueba plena. Esto es, los indicios -elementos esenciales constituidos por hechos y circunstancias ciertas- se utilizan como la base del razonamiento lógico del juzgador para considerar como ciertos, hechos diversos de los primeros, pero relacionados con ellos desde la óptica causal o lógica. Ahora bien, un requisito primordial de dicha prueba es la certeza de la circunstancia indiciaria, que se traduce en que una vez demostrada ésta, es necesario referirla, según las normas de la lógica, a una premisa mayor en la que se contenga en abstracto la conclusión de la que se busca certeza. Consecuentemente, al ser el dolo un elemento que no puede demostrarse de manera directa- excepto que se cuente con una confesión del sujeto activo del delito- para acreditarlo, es necesario hacer uso de la prueba circunstancial que se apoya en el valor incriminatorio de los indicios y cuyo punto de partida son hechos y circunstancias ya probados.

4.2. Artículo 211 BIS 2

PARA EL ARTÍCULO 211 BIS 2, DENTRO DEL CUAL SE CONTIENE LA HIPÓTESIS NORMATIVA DESCRIBIENDO LO SIGUIENTE:

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o

impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

A) Con relación al primero y segundo párrafo del tipo penal en cuestión, se encuentran las hipótesis de modificar, de destruir, de provocar la pérdida, de conocer y de copiar la información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, éstas se actualizarán, básicamente haciendo el mismo estudio realizado en párrafos anteriores con respecto del artículo 211 Bis 1, sólo que aquí aparece el Estado como una calidad específica del Sujeto Pasivo, por lo que se adicionará la acreditación de los siguientes elementos:

ELEMENTOS OBJETIVOS

El sujeto pasivo, quien a decir de Miguel Ángel Aguilar, la doctrina ha separado en dos vertientes, por un lado es considerado como quien resiente la conducta descrita por el tipo, y por otro lado es considerado como el titular del bien jurídico lesionado o puesto en peligro; asimismo se le denomina víctima. Por otro lado Gustavo Malo Camacho lo conceptualiza como la persona física o moral, titular del bien jurídico protegido, lesionado o puesto en peligro, por la conducta típica, que genera la violación al deber contenido en la prohibición o mandato previsto en el tipo penal:

Sujeto pasivo calidad. Algunos tipos delictivos exigen una cierta calidad específica, sin la cual, el delito de que se trate no podría producirse. Debe distinguirse, aquí, entre los conceptos del sujeto pasivo y de la víctima u ofendido del delito. Aun cuando frecuentemente son coincidentes, no siempre acontece así. Víctima es la persona física que resulta directamente afectada por la conducta que causa la lesión al bien jurídico, sin que ello sea obstáculo para reconocer como posible sujeto pasivo aun tercero que resultara ser el titular del bien jurídico. (V.gr.: el empleado que regresa con la nomina y es asaltado, sufre el acto de robo y el desapoderamiento del dinero objeto del ilícito y, por tanto, es la víctima de un robo, pero es evidente que el sujeto pasivo lo será el patrón o la empresa de la que aquél es solo un empleado, y por tanto no sufre el perjuicio económico que si afecta al bien jurídico, patrimonio, de la empresa quien es por tanto el sujeto pasivo). En un delito de homicidio, la víctima es la persona que sufre la acción homicida y

que, por lo mismo, al fallecer deja de ser persona para constituirse en cadáver, jurídicamente mencionado como el "occiso" o el de cujus y que, en términos de análisis de la conducta típica, será el objeto material del delito, pero sujeto pasivo del delito, serán los familiares que son titulares de los bienes jurídicos tutelados y, por tanto, quienes tienen el derecho de hacer las reclamaciones correspondientes.[95]

En este tenor, la Ley General de Víctimas, publicada en el Diario Oficial de la Federación el 9 de enero de 2013, determina que se denominarán víctimas directas aquellas personas físicas que hayan sufrido algún daño o menoscabo económico, físico, mental, emocional, o en general cualquiera puesta en peligro o lesión a sus bienes jurídicos o derechos como consecuencia de la comisión de un delito.

No obstante, que esta ley no contempla al Estado como víctima después de que existe un daño consiste fundamentalmente en una lesión al patrimonio público, representada en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes o recursos públicos o de los intereses patrimoniales del Estado, consecuentemente en adición a los bienes jurídicos que la norma tutela y que el mismo Código penal establece como la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Ahora bien, además de la calidad de Estado como Sujeto Pasivo del tipo penal en estudio, también se agrega a éste como elemento normativo, toda vez que, como expresión semántica tiene varias connotaciones interpretativas, donde en el aspecto doctrinal para definir el concepto de Estado han surgido a la vez diversas teorías[96] que intentan explicar el significado, entre las cuales destacan las teorías organicistas, sociológicas, jurídicas y teorías que lo explican a través de los elementos que lo integran; la teoría jurídica ha determinado que se clasifican en dos grupos: la primera sostienen la personalidad jurídica del Estado y la segunda identifica al Estado como unidad entre el Estado y el derecho.

---

[95] Malo Camacho, Gustavo*, Derecho penal mexicano,* quinta edición, editorial Porrúa, México 2003, p.340.

[96] Pichardo Pagaza, Ignacio, *Introducción a la nueva administración pública de México, Volumen 1*, Instituto Nacional de Administración Pública, segunda edición, corregida y aumentada, México, abril 2002, p.14

La teoría de la personalidad jurídica afirma que el Estado es una persona como unidad o ente jurídico, apareciendo como base del derecho público; mientras que como unidad Estado y Derecho, el Estado es un sistema de normas o la expresión para designar la unidad de tal sistema y no puede ser más que el orden jurídico o la expresión de su unidad, con ella se alude a la voluntad de los integrantes de una colectividad de regir sus actos y conductas con apego a las normas jurídicas en vigor. La teoría que explica al Estado a través de sus elementos sugiere que uno de ellos es el poder público y sus órganos, la expresión única del poder público del Estado es la Constitución, como tercer elemento de los órganos de ese poder público se encuentra la administración pública. Por otro lado, como una interpretación normativa del Estado, de conformidad con el artículo 41, con relación al 49, 50, 80 y 94 de la CPEUM en su última reforma publicada DOF 24-02-2017, especifica que, el pueblo mexicano ejerce su soberanía por medio de los Poderes de la Unión, en los casos de la competencia de éstos, y por los de los Estados y la Ciudad de México, resaltando la jerarquía de autoridades federales y autoridades locales; asimismo, el Supremo Poder de la Federación se divide para su ejercicio en Legislativo, Ejecutivo y Judicial; el poder legislativo se deposita en un Congreso general, el ejercicio del Supremo Poder Ejecutivo se deposita en un Presidente de la república y que el ejercicio del Poder Judicial se deposita en la Suprema Corte de Justicia, en un Tribunal Electoral, en Tribunales colegiados de circuito, en Tribunales unitarios de circuito y en Juzgados de Distrito; en consecuencia, la misma constitución ordena que la Administración Pública Federal será centralizada y paraestatal conforme a la Ley Orgánica que expida el Congreso, que distribuirá los negocios del orden administrativo de la Federación que estarán a cargo de las Secretarías de Estado y definirá las bases generales de creación de las entidades paraestatales y la intervención del Ejecutivo Federal en su operación.

Consecuentemente, para vincular el elemento material del delito, como el patrimonio, propiedad del Estado, se define que los elementos de este patrimonio son dos: i) Activo, constituido por el conjunto de bienes y derechos y ii) Pasivo, comprendido por las cargas y obligaciones susceptibles de apreciación pecuniaria;

asimismo, los elementos del patrimonio del Estado, como consecuencia de su personalidad jurídica, son el conjunto de bienes, recursos, inversiones y demás derechos sobre las cosas que integran el dominio público y privado de la Federación: a) que se valoran económicamente, b) afectados a una finalidad pública, interés general o utilidad pública, que se traduce en la prestación de servicios a cargo del Estado y c) que forman una unidad de la cual el Estado o las entidades públicas creadas por él, son titulares.

De esta forma, el patrimonio del Estado está sujeto fundamentalmente a un régimen de derecho Público, basado en las disposiciones de los artículos 27 y 42 a 48 de la Constitución, ese régimen no está sistematizado y unificado, sino que está integrado por muchísimas leyes derivadas de párrafos o fracciones del mismo artículo 27, dentro de los cuales se consideran como bienes patrimoniales: I) aquellos bienes que se mantienen en un patrimonio administrativo única y exclusivamente por razón de su rendimiento económico o por la garantía que tal inversión económica supone, II) bienes que las entidades administrativas poseen como instrumentos para el desarrollo de actividades que, no obstante su utilidad pública, están sometidos en bloque a las formas de derecho Privado, III) bienes que, a pesar de estar afectos a un servicio público, se regulan por un régimen jurídico positivo esencialmente análogo al de la propiedad civil o que, a falta de reglas expresas, debe entenderse que la titularidad administrativa está suficientemente garantizada con el régimen de la propiedad civil.

B) Con relación al tercer párrafo del tipo penal en cuestión, se encuentran las hipótesis de conocer, obtener, copiar o utilizar información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, las cuales se acreditarán con los siguientes elementos:

ELEMENTOS OBJETIVOS

Con relación a los elementos objetivos, al realizar la conducta típica, con la acreditación de la acción material de *conocer*, *obtener*, *copiar* o *utilizar* cualquier información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos; dicha información puede estar representada materialmente en cualquiera de sus diferentes formatos, ya sea en archivo, video, audio o gráfica y además, almacenada dentro de cualquier dispositivo internos o periféricos del sistema informático, destinados para tal fin, como memorias de estado sólido semiconductor conocidas como ROM y RAM, unidades mecánicas de grabación magnética conocidas como Disco Duro, unidades de disco compacto que utilizan rayos láser para leer información conocidos como CD ROM, unidades de almacenamiento externa, tipo lápiz que utiliza memoria flash conocidas como USB, o unidades de almacenamiento con formato de tarjeta de memoria para dispositivos portátiles conocida como SD.

Con la actualización de estas conductas de acción se lesiona el bien jurídico tutelado que la ley penal mexicana protege y está definida como “acceso ilícito a sistemas y equipos de informática”; así como los bienes jurídicamente tutelados señalados en la Convención de Budapest sobre Ciberdelincuencia concerniente a la “confidencialidad”, la “integridad” y la “disponibilidad” de los datos y sistemas informáticos. Porque así lo requiere el tipo penal, la calidad del sujeto activo, debe ser cualquier persona que no tenga autorización, dicha autorización la otorga el propietario o el administrador del sistema informático; además de que en el contexto de la ingeniería de seguridad informática, la autorización es una parte del mismo sistema operativo que protege los recursos del sistema permitiendo, a través de contraseñas, que sólo sean usados por aquellos consumidores a los que se les ha concedido autorización para ello.

El objeto material sobre el que recaen las conductas típicas de conocer, obtener, copiar o utilizar lo constituye la información que en forma de datos electrónicos está contenida en las unidades de almacenamiento del sistema o equipo informático; esta información debe ser de manera rigurosa la que determina la

CPEUM en su última reforma publicada DOF 24-02-2017, artículo 21 inciso b), al establecer que el Sistema Nacional de Seguridad Pública, estará sujeto a las siguientes bases mínimas con relación de las bases de datos criminalísticos y de personal para las instituciones de seguridad pública.

Con respecto de los medios comisivos, el tipo penal no requiere el medio específico para la consumación del hecho, esto es, que para conocer, obtener, copiar o utilizar información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, puede ser el acceso en el mismo sistema en forma local, en la misma computadora o bien a través de la red local o de internet.

Referente a la circunstancias de tiempo, modo, lugar y ocasión, solo refiere el tipo penal que se actualiza el supuesto, en el momento en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, entendido éste como firewall, antivirus, filtros de tráfico de red, reglas de filtrado de patrones, políticas permisivas o restrictivas, un sistema de detección de intrusos o IDS, etcétera.

ELEMENTOS NORMATIVOS

Para los elementos normativos, se presentan cuatro expresiones semánticas a saber: *autorización*, *información*, *sistemas, equipo o medio de almacenamiento informático*, así como los verbos rectores de *conocer*, *obtener*, *copiar* o *utilizar* y la expresión *seguridad pública.*;

Donde la expresión *autorización*, deriva de una interpretación doctrinal, como un acto de naturaleza judicial, administrativa o, simplemente privado, en virtud del cual una persona queda facultada para ejercer determinado cargo o función o para realizar determinado acto de la vida civil.

Mientras que la *información* debe provenir de una interpretación meramente jurídica dada la categoría de información que la CPEUM en su última reforma

publicada DOF 24-02-2017, artículo 21 enfatiza con relación de las bases de datos criminalísticos y de personal para las instituciones de seguridad pública; asimismo la actual Ley General del Sistema Nacional de Seguridad Pública, reglamentaria del artículo 21 de la Constitución en materia de Seguridad Pública, en su última reforma publicada DOF 26-06-2017, establece en la fracción segunda del artículo quinto, el concepto legal de la información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública:

> *Artículo 5.- Para los efectos de esta Ley, se entenderá por:*
>
> *I. …*
> *II. Bases de Datos Criminalísticas y de Personal: Las bases de datos nacionales y la información contenida en ellas, en materia de detenciones, información criminal, personal de seguridad pública, servicios de seguridad privada, armamento y equipo, vehículos, huellas dactilares, teléfonos celulares, sentenciados y las demás necesarias para la operación del Sistema.*

En tanto que para la frase *sistemas, equipo o medio de almacenamiento informáticos*, necesariamente merece una interpretación doctrinal y cultural, toda vez que se refiere a los desarrollos científicos que el ser humano ha realizado como medio de mejorar su desempeño en cualquier aspecto de la vida, y que ahora las instituciones de seguridad pública las utilizan para optimizar su labor como servidores públicos al servicio del Estado, por lo que se puede definir como sistema o equipo informático aquel instrumento de naturaleza electrónica destinada para procesar información o datos electrónicos para lo cual se estructura en dos grupos: 1. Hardware compuesto de: i) c.p.u (Unidad Central de Proceso), ii) monitor, iii) teclado, iv) mouse, v) impresora, vi) modem para acceso a internet, etcétera; 2. Software compuesto de: i) firmware, ii) sistemas operativos y iii) aplicaciones.

Para describir brevemente en qué consisten los últimos tres elementos concernientes al software, se tiene que el firmware es el conjunto de instrucciones necesarias para el buen funcionamiento del computador; también es llamado

Programa de arranque; los sistemas operativos son los programas que administran los dispositivos y recursos del computador v.g.: Windows, Linux, Mac, Unix; en tanto que las aplicaciones son programas para tareas específicas tales como Word (para escribir textos), Excel (para crear tablas, gráficas), Internet Explorer (para navegar en Internet).

Los medios de almacenamiento se relacionan con cualquier dispositivo informático destinado para almacenar información y que para especificar con precisión se enlistan las siguientes: 1. Dispositivos magnéticos como: i) unidad de cinta magnética, ii) unidad de disco flexible o disquetera, iii) unidad de disco rígido o disco duro; 2. Dispositivos ópticos: i) unidad de CD-ROM o lectora de CD, ii) unidad de CD-R/RW, iii) grabadora o regrabadora de CD-R/RW, iv) unidad de DVD-ROM o lectora de DVD, v) unidad de DVD-R/RW o grabadora de DVD±R/RW, vi) unidad de base de datos, vii) lectora o grabadora de discos Blu-ray; 3. Unidad de disco magneto-óptico: i) unidad Zip, ii) unidad Jaz, iii) unidad Super Disk, Orb Drive; 4. Unidad de estado sólido: i) unidad de memoria flash y ii) unidad de tarjetas de memoria.

Con respecto de los verbos rectores, de *conocer*, *obtener*, *copiar* o *utilizar,* los cuales son términos meramente doctrinales y que el diccionario de la real academia española lo define como:

> ***Conocer*** es entender, advertir, saber, percibir, averiguar por el ejercicio de las facultades intelectuales la naturaleza, cualidades y relaciones de las cosas.
>
> ***Copiar*** es reproducir una obra exactamente igual o muy parecida que otra.
>
> La expresión ***obtener****,* la cual proviene del latín *obtinēre* que significa tener, alcanzar, conseguir y lograr algo que se merece, solicita o pretende.
>
> La expresión ***utilizar****,* en el contexto de los sistemas de información, es hacer que algo sirva para un fin.

La última expresión semántica que contiene la descripción típica es *seguridad pública*, la cual se desprende de una interpretación completamente legal, así la

misma Ley General del Sistema Nacional de Seguridad Pública, en su última reforma publicada DOF 26-06-2017, considera que la *seguridad pública* es una función a cargo de la Federación, las entidades federativas y municipios, además de que tiene como fines el salvaguardar la integridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos y comprende la prevención especial y general de los delitos, la sanción de las infracciones administrativas, así como la investigación y la persecución de los delitos y la reinserción social del sentenciado.

ELEMENTOS SUBJETIVOS

La acreditación del elemento subjetivo genérico de la conducta al tipo, es de carácter doloso en su modalidad de dolo directo, toda vez que, en este tipo de delitos el sujeto activo cumple con el elemento cognoscitivo al conocer los elementos del tipo penal, y el elemento volitivo al querer el resultado típico del hecho descrito por la ley, el cual es la destrucción de la información; estos elementos se ratifican de manera fáctica cuando el sistema o equipo de cómputo cuestiona sobre la destrucción de la información y además, por tratarse de daños en propiedad ajena.

Es de especial importancia señalar que dentro de este tercer párrafo del artículo 211 Bis 2, se contiene una segunda hipótesis, que especifica la calidad del sujeto activo de la conducta de la siguiente forma: *Si el responsable es o hubiera sido servidor público en una institución de seguridad pública.*

En consecuencia, se desprende como elemento normativo del delito para ser acreditado, la expresión semántica específica de *servidor público de una institución de seguridad pública*; y que ésta se encuentra acotada a la persona que ejerce o ejercía la función de seguridad pública; a través del método deductivo, abordaré el concepto genérico de servidor público hasta llegar a la de servidor público de una institución de seguridad pública; ya el artículo 108 de la CPEUM,

reputa como servidores públicos a los representantes de elección popular, a los miembros del Poder Judicial de la Federación, los funcionarios y empleados, y, en general toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en la Administración Pública Federal; asimismo, las Constituciones de los Estados de la República y de la Ciudad de México, precisan, para efectos de sus responsabilidades, el carácter de servidores públicos de quienes desempeñen empleo, cargo o comisión en los Estados y en los Municipios.

En este orden de ideas, se puede inferir que se considera un servidor público a cualquier persona a la que el Estado le haya conferido un cargo o una comisión de cualquier índole, es decir, persona física que realiza una función pública de cualquier naturaleza.

Así mismo, en términos de numeral 2 con relación al 3 y 4 de Ley General del Sistema Nacional de Seguridad Pública, se entiende que la seguridad pública es una función, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos; además comprende la prevención especial y general de los delitos, la sanción de las infracciones administrativas, la investigación y la persecución de los hechos constitutivos de delito.

Esta función pública, se realizará en los diversos ámbitos de competencia por conducto de las instituciones policiales, de las instituciones de procuración de justicia, de las instituciones de las instancias encargadas de aplicar las infracciones administrativas, de las instituciones de la supervisión de medidas cautelares, de las instituciones de suspensión condicional del procedimiento de los responsables de la prisión preventiva y ejecución de penas.

Por otro lado, el Sistema Nacional de Seguridad Pública contará para su funcionamiento y operación con las instancias, instrumentos, políticas, acciones y servicios suficientes para cumplir con los fines de la seguridad pública.

C) Con relación al cuarto párrafo del tipo penal en cuestión, se encuentran las hipótesis que agravan la punibilidad, esto es sí: **1)** *la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración de justicia,* ***2)*** *la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la impartición de justicia, y* ***3)*** *la conducta recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes;* estas tres hipótesis se acreditarán con los siguientes elementos:

1) La acreditación de los elementos objetivos, porque así lo requiere el tipo penal, relacionados con las circunstancias de tiempo, modo, lugar y ocasión, que para el tipo en estudio, refiere a las formas de realización de la conducta, es decir, que dichas conductas consisten en retardar o entorpecer la procuración de justicia, en agravio de las víctimas de los delitos.

La procuración de justicia implica[97] la tarea de asegurar el cumplimiento de la normas jurídicas, y al no estar circunscrita únicamente al ámbito penal y a la persecución de los delitos, sino que, en múltiples aspectos, defiende los intereses de la sociedad y de los grupos sociales desprotegidos.

En artículo 102 de la CPEUM, mandata que corresponde al Ministerio Público de la Federación la persecución, ante los tribunales, de todos los delitos del orden federal; procurará que los juicios federales en materia penal se sigan con toda regularidad para que la impartición de justicia sea pronta y expedita; pedirá la aplicación de las penas, e intervendrá en todos los asuntos que la ley determine.

En este tenor, también las Constituciones de los Estados y del la Ciudad de México, garantizarán que las funciones de procuración de justicia se realicen con base en los principios de autonomía, eficiencia, imparcialidad, legalidad, objetividad, profesionalismo, responsabilidad y respeto a los derechos humanos; además la Ley Orgánica de la Procuraduría General de Justicia del Distrito Federal, ahora Ciudad de México publicada en el Diario Oficial de la Federación el

[97] Ojeda Paullada, Pedro, *Concepto de Procuraduría*, Instituto Nacional de Administración Pública, Núm. 97 revista de administración pública, México, 1998. Consulta en línea. http://historico.juridicas.unam.mx/publica/librev/rev/rap/cont/97/pr/pr2.pdf

20 de junio de 2011, establece que la institución del Ministerio Público, estará a cargo del Procurador General de Justicia y que sus atribuciones la ejercerá por sí, o a través de los agentes del Ministerio Público, de la Policía de Investigación, de los Peritos y demás servidores públicos en el ámbito de su respectiva competencia.

En resumen, la vigilancia de la legalidad y la promoción de la pronta, expedita y debida procuración e impartición de justicia, comprenden el dar a conocer a las autoridades competentes aquellos hechos no constitutivos de delito, que hubieren llegado al conocimiento del Ministerio Público; además de conocer de las quejas por demoras, excesos y faltas de los agentes del Ministerio Público, de la Policía de Investigación, oficiales secretarios y peritos, iniciando los procedimientos legales que correspondan en los términos fijados por las normas reglamentarias y demás disposiciones aplicables.

Otra función del Procurador es ejercer inspección, supervisión y vigilancia en todas las unidades del Ministerio Público, Policía de Investigación y peritos, así como ordenar operativos de supervisión, visitas, estudios o análisis, monitoreo y demás medios de control e inspección;

Por todo lo anterior, el elemento objetivo de la conducta del tipo en análisis se actualiza al acreditar la obstrucción o evitar el cumplimiento de las actividades que implican la procuración de justicia señaladas, sí y sólo sí, se haya acreditado cualquiera de las hipótesis planteadas en el párrafo primero, segundo o tercero del artículo 211 Bis 2, en los siguientes términos:

> *Al que sin autorización conozca, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos o medio de almacenamiento de informática del Estado o de seguridad pública, protegidos por algún mecanismo de seguridad*.

2) La acreditación de los elementos objetivos, porque así lo requiere el tipo penal relacionados con las circunstancias de tiempo, modo, lugar y ocasión, que para el tipo en estudio, refiere a las formas de realización de la conducta, es decir, que dichas conductas consisten en retardar o entorpecer la impartición de justicia.

La impartición de justicia es una de las prioridades fundamentales de todo Estado de derecho, para garantizar la paz y la seguridad ciudadana, luego entonces, toda persona tiene derecho a que se le administre justicia por tribunales de manera pronta, completa e imparcial.

La CPEUM en su artículo 95, ordena que se deposita el ejercicio del poder judicial de la federación en una Suprema Corte de Justicia; asimismo la Ley Orgánica del Poder Judicial de la Federación, con su última reforma publicada DOF 19-06-2017, determina que el poder judicial de la federación se ejerce por la Suprema Corte de Justicia de la Nación, el tribunal electoral, los tribunales colegiados de circuito, los tribunales unitarios de circuito, los juzgados de distrito, el consejo de la judicatura federal, el jurado federal de ciudadanos y los tribunales de los Estados y de la ciudad de México.

Por ejemplo, la Ley Orgánica del Tribunal Superior de Justicia del Distrito Federal, hoy Ciudad de México, con su última reforma publicada en la Gaceta Oficial del Distrito Federal el 02 de junio de 2015, establece que el ejercicio jurisdiccional en todo tipo de asuntos civiles, mercantiles, penales, de extinción de dominio, familiares y los del orden federal en los casos que expresamente las leyes les confieran jurisdicción, corresponde a los servidores públicos y órganos judiciales que se señalan a continuación: Magistrados del Tribunal Superior de Justicia del Distrito Federal y Jueces del Distrito Federal.

De tal suerte que, por lo que hace al elemento objetivo de la conducta del tipo en análisis se actualiza al acreditar la obstrucción o evitar el cumplimiento de las actividades que implican la impartición de justicia señaladas, si y sólo si se haya acreditado cualquiera de las hipótesis planteadas en el párrafo primero, segundo o tercero del artículo 211 Bis 2, en los siguientes términos:

Al que sin autorización conozca, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos o medio de almacenamiento de informática del Estado o de seguridad pública, protegidos por algún mecanismo de seguridad.

3) La acreditación de los elementos objetivos, porque así lo exige el tipo penal, relacionados con el objeto material que ahora adquiere una calidad específica, es decir que la conducta de acción de conocer o copiar o modificar o destruir o provocar la pérdida de información o equipo informático, y que esta información sean estrictamente los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

Para esto la Ley General del Sistema Nacional de Seguridad Pública, con su última reforma publicada DOF 26-06-2017, establece la conformación del Centro Nacional de Información CNI, el cual es el responsable de la operación del Sistema Nacional de Información de Seguridad Pública, que además de administrar y resguardar las bases de datos criminalísticos y de personal del sistema, suministrará la información a los tres órdenes de gobierno, porque sus bases de datos se integran con la información proporcionada por la federación, los estados, la Ciudad de México y los municipios, con base en sus propios registros y datos bajo su resguardo.

Así mismo, el CNI realiza la homologación de los registros y el intercambio de datos, vigilando la seguridad de las bases y el cumplimiento de los criterios para el acceso y actualización de las mismas.[98]

Por consiguiente, el Centro Nacional de Información es la autoridad competente para el resguardo de la información de los registros relacionados con un procedimiento penal.

[98] Del Río Hernández, Guillermo, *Centro Nacional de Información*, Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública. https://www.gob.mx/sesnsp/estructuras/dr-ricardo-corral-luna. Consulta en línea. 30 de Julio 2017 07:30.

En este orden de ideas, para acreditar el cuarto párrafo del 211 Bis 2, también se debe acreditar el elemento normativo que surge del legislador, referente a la expresión *registro del procedimiento penal*. Para esto acudimos a la interpretación que la propia normatividad proporciona.

Así, el Código Nacional de Procedimientos Penales con su última reforma publicada DOF 17-06-2016 establece que el procedimiento penal comprende las siguientes etapas: I) la etapa de investigación, que a su vez comprende las siguientes fases: a) la investigación inicial, que comienza con la presentación de la denuncia, querella u otro requisito equivalente y concluye cuando el imputado queda a disposición del Juez de control para que se le formule imputación, y b) la investigación complementaria, que comprende desde la formulación de la imputación y se agota una vez que se haya cerrado la investigación; II) la etapa intermedia o de preparación del juicio, que comprende desde la formulación de la acusación hasta el auto de apertura del juicio, y III) La etapa de juicio, que comprende desde que se recibe el auto de apertura a juicio hasta la sentencia emitida por el tribunal de enjuiciamiento.

Luego entonces, los registros, que aduce la norma, deben contener información precisa relacionada con cada una de las fases y etapas comprendidas en el procedimiento penal vigente; asimismo, los registros resguardados por el Centro Nacional de Información, contienen información penitenciaria, el de personal de seguridad pública, el de vehículos robados y recuperados, el de personas extraviadas o desaparecidas, así como los provenientes del informe policial homologado y de los reportes de incidencia delictiva y víctimas del delito.

En resumen, las bases de datos del sistema nacional de información sobre seguridad pública contribuyen con información útil para la política de seguridad pública, ayudan a combatir el delito y a fortalecer la justicia, pues como dice su titular, son consultadas tanto por instituciones de seguridad pública como por autoridades de procuración e impartición de justicia a nivel nacional.

4.3. Artículo 211 BIS 1 Y BIS 3.

PARA EL ARTÍCULO 211 BIS 3, DENTRO DEL CUAL SE CONTIENE LA HIPÓTESIS NORMATIVA DESCRIBIENDO LO SIGUIENTE:

> *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.*

Con relación al primer del tipo penal, se acreditará con los elementos siguientes:

ELEMENTOS OBJETIVOS

Con la materialización de la conducta tipificada en la ley penal, la cual consiste en la acción de hecho de forma voluntaria de modificar, destruir o provocar la pérdida de información contenida en los sistema o equipo informáticos, ya se ha abundado sobre la calidad, características y naturaleza de la información en los estudios referente a los tipos contenidos en los artículos 211 Bis 1 y 211 Bis 2.

Mediante esta conducta de acción también se lesiona vulnera y menoscaba el bien jurídico tutelado que la Convención de Budapest contra la ciberdelincuencia define como la *confidencialidad*, la *integridad* y la *disponibilidad* de los datos y sistemas informáticos.

Porque así lo requiere el tipo penal, la calidad del sujeto activo y del pasivo; para el caso que nos ocupa los dos sujetos partícipes del tipo si requieren la calidad específica, por un lado para el sujeto activo debe ser una persona autorizada, mientras que para el sujeto pasivo es el Estado, en los estudios anteriores ya se abordó el tema de la autorización y el Estado como sujeto pasivo del tipo penal.

> *También es acertado advertir que en esta conducta punible están inmersos quienes tienen potestad, autorización o posibilidad de acceder al sistema informático, en forma legal o reglamentaria, pero que ingresa a las redes más allá de lo permitido, o acordado y lo hacen sin sujeción a lo pactado, convenido o estipulado en las diversas disposiciones existentes en las instituciones públicas como privadas que manejan la información automatizada, cuando ese acceso se hace en forma alargada e inconsulta, violando el perfil asignado para introducirse en el sistema informático, de contera vulnera la confidencialidad, la integridad y la disponibilidad de los datos.*[99]

El objeto material está constituido por la información de tipo informático del sistema o equipo en cuestión, así como sus características específicas como: formatos, tipos e importancia.

Con respecto de los medios comisivos, el tipo penal no requiere un medio específico para la consumación del hecho. Referente a la circunstancias de tiempo, modo, lugar y ocasión, solo refiere el tipo penal que se actualiza el supuesto, en el momento en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, también ya se abundó lo referente a los mecanismos de seguridad informática.

[99] Palomá Parra, Luis Orlando, op. cit. nota 21, p.83.

ELEMENTOS NORMATIVOS

Se presentan cuatro expresiones semánticas a saber: *autorización*, *información*, *sistemas u equipo de informática y Estado;* además de los verbos rectores *modificar, destruir y provocar pérdida.*

La interpretación para la *autorización*, en el caso que nos ocupa debe desprenderse de la norma jurídica por la calidad del sujeto activo toda vez que el Estado a través de sus instituciones de gobierno federales, estatales o municipales serán quien otorgan esta autorización, por ser éste un acto de naturaleza judicial o administrativa, en virtud del cual una persona queda facultada para ejercer determinado cargo o función.

La *información* puede provenir de un aspecto cultural y legal; la información está expresada en cualquier modo, sea alfabética, numérica, gráfica, fotográfica o sonora, por citar algunas, y puede estar contenida en cualquier soporte como en papel, en la memoria de un equipo informático, en una cinta de video o en un dvd.

Por otro lado, con respecto de la expresión *sistema o equipo de cómputo,* se relaciona a los instrumentos creados por el ser humano como herramienta, con diferentes usos: educativos, de comunicación, de trabajo, de entretenimiento, etcétera.

Con relación a los verbos rectores *modificar,* es hacer una cosa diferente de como era antes, alterar, enmendar, reformar o transformar una cosa alterando sus características; *destruir*, es reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño, deshacer o inutilizar algo; y la expresión *causar la pérdida*, se desprende de la doctrinal y se entiende como producir cierto efecto o dar lugar a cierta consecuencia que en este caso es la pérdida irreparable de la información o datos contenidos dentro del sistema o equipo informático.

> *...se refiere al daño en bien ajeno "el que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble...". Lo que prohíbe el codificador en este delito es todo lo referente al daño que se le puede ocasionar al almacenamiento de la información o al sistema de información que contienen los datos informáticos, la destrucción, el menoscabar, suprimir, deteriorar, alterar, modificar,*

eliminar, suprimir, deteriorar, alterar, modificar, eliminar los datos informáticos, básicamente todo lo referente, se redunda, a dañar el software o el hardware ajenos.[100]

ELEMENTOS SUBJETIVOS

Solo se contiene el elemento genérico, el carácter doloso de la conducta en su modalidad de dolo directo, desde luego que en este tipo de delitos el sujeto activo cumple con el elemento cognoscitivo al conocer de los elementos del tipo penal, y el elemento volitivo al querer el resultado típico del hecho descrito por la ley, el cual es la modificación, destrucción o causar la pérdida de la información; estos elementos se ratifican de manera fáctica cuando el sistema o equipo de cómputo cuestiona sobre la destrucción de la información y sobre todo cuanto se sabe que la información es de vital importancia para la persecución de los delitos.

Es interesante advertir con respecto del acceso a la información pública en poder del Estado, toda vez que, la misma CPEUM en su artículo 6º reconoce que toda persona tiene derecho al libre acceso a información plural y oportuna como ejercicio del derecho de acceso a la información; asimismo, la Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 4 de mayo de 2015, establece los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios; todo esto través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como garante del derecho humano de acceso a la información, el cual comprende el solicitar, investigar, difundir, buscar y recibir información.

[100] Ibídem, p.93

Luego entonces, toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, la Ley Federal, las leyes de las Entidades Federativas y la normatividad aplicable en sus respectivas competencias; pero ojo, sólo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público y seguridad nacional, en los términos dispuestos por la misma Ley.

La clasificación de la información es el proceso mediante el cual el Estado determina que la información en su poder actualiza alguno de los supuestos de reserva o confidencialidad: i) información reservada, es la que comprometa la seguridad nacional, la seguridad pública o la defensa nacional o pueda poner en riesgo la vida, seguridad o salud de una persona física; también la que obstruya la prevención o persecución de los delitos, obstruya los procedimientos para fincar responsabilidad a los Servidores Públicos, afecte los derechos del debido proceso, vulnere la conducción de los Expedientes judiciales o se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público; y ii) información confidencial, es la que contiene datos personales concernientes a una persona identificada o identificable.

Los Documentos clasificados como reservados serán públicos cuando se extingan las causas que dieron origen a su clasificación.

Materialmente, cualquier persona por sí misma o a través de su representante, podrá presentar solicitud de acceso a información ante la Unidad de Transparencia, a través de la Plataforma Nacional, en la oficina u oficinas designadas para ello, vía correo electrónico, correo postal, mensajería, telégrafo, verbalmente o cualquier medio aprobado por el Sistema Nacional.

4.4. Artículo 211 BIS 4, BIS 5 Y BIS 6.

PARA EL ARTÍCULO 211 BIS 4 PRIMER PÁRRAFO Y 211 BIS 5 PRIMER PÁRRAFO, CON RELACION AL 211 BIS 6, DENTRO DEL CUAL SE CONTIENE LA HIPÓTESIS NORMATIVA DESCRIBIENDO LO SIGUIENTE:

> *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.*

> *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.*

El tipo penal se actualizará en el momento de acreditar todos y cada uno de los elementos objetivos, normativos y subjetivos:

ELEMENTOS OBJETIVOS

La hipótesis que conforman los dos párrafos que integran este tipo penal, invariablemente se materializa con todos los actos idóneos de ejecución para que de manera voluntaria y mediante cualquiera de las conductas señaladas se cause, como resultado material, modificar, destruir o provocar la pérdida de la información contenida en un sistema o equipo de informática.

Con estas conductas de acción se lesionan los bienes jurídicos tutelados que la norma penal mexicana y la Convención de Budapest contra la ciberdelincuencia han definido como: la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

Porque así lo requiere el tipo penal, la calidad del sujeto activo por un lado para el 211 Bis 4, debe ser cualquier persona que no tenga autorización y por otro lado, para el 211 Bis 5, debe ser cualquier persona que esté autorizada, de manera general la autorización la otorgan las entidades financieras integrantes del Sistema Financiero Mexicano tanto a sus empleados como a los usuarios de servicios financieros, esto de conformidad con su reglamento interno y como una garantía constitucional de acceso a la información.

El objeto material sobre el que recae la conducta lesiva está constituido por la información contenida en los elementos estructurales encargados de resguardar los datos dentro del sistema o equipo informático al que pertenece las bases de datos relativas a operaciones y servicios de las entidades o de segmentos de los mercados del sistema financiero.

En cuanto a los medios comisivos, el tipo penal no requiere el medio específico para la consumación del hecho, esto es, que para modificar, destruir o provocar la pérdida de la información contenida en un sistema o equipo informático, ésta puede ser de cualquier manera, es decir, accediendo al sistema localmente.

Referente a la circunstancias de tiempo, modo, lugar y ocasión, el ilícito se actualizará en la ocasión misma en que el equipo informático se encuentre protegido por algún mecanismo de seguridad, entendida como seguridad informática la que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

> *El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas. Para el conglomerado social la seguridad de la información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo y de los datos personales que se encuentran resguardos como información privada.*
>
> *Seguridad de la información ha evolucionado considerablemente convirtiéndose en una carrera acreditada a nivel ecuménico. Este campo ofrece muchas áreas de especialización, incluidas la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión*

de seguridad, entre otras.[101]

ELEMENTOS NORMATIVOS

Concurren las expresiones: autorización, información, instituciones que integran el sistema financiero y los verbos rectores: modificar, destruir o provocar la pérdida.

Con respecto de la *autorización*, ésta derivada de una interpretación doctrinal, y que dentro del contexto de la informática es aquel usuario autorizado, en materia de informática, se define como aquella persona física o moral, que en forma eventual o permanente tiene acceso a algún servicio público o privado de telecomunicaciones y con relación a los usuarios de servicios financieros tendrán autorización siempre y cuando así se hubiere pactado con la institución de crédito, hará su manifestación a través de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos.

Referente a la *información*, para el caso que nos ocupa proviene de una interpretación legal toda vez que tanto la Ley de la Comisión Nacional Bancaria y de Valores, con su última reforma publicada DOF 10-01-2014, así como la Ley de Instituciones de Crédito, con su última reforma publicada DOF 17-06-2016; las cuales establecen el tipo de información sobre clientes, cuentas u operaciones de las instituciones de crédito emisoras de cualquiera de los objetos como tarjetas de crédito, de débito, cheques, formatos o esqueletos de cheques o en general cualquier otro instrumento de pago, de los utilizados o emitidos por instituciones sistema financiero mexicano.

En relación con las instituciones que integran el sistema financiero la Ley de la Comisión Nacional Bancaria y de Valores, proporciona la lista de las entidades financieras integrantes del Sistema Financiero Mexicano, a saber: Sociedades controladoras de grupos financieros, instituciones de crédito, casas de bolsa,

[101] Palomá Parra, Luis Orlando, op. cit. nota 21, p.147

especialistas bursátiles, bolsas de valores, sociedades de inversión, sociedades operadoras de sociedades de inversión, sociedades distribuidoras de acciones de sociedades de inversión, almacenes generales de depósito, uniones de crédito, arrendadoras financieras, empresas de factoraje financiero, sociedades de ahorro y préstamo, casas de cambio, sociedades financieras de objeto limitado, sociedades financieras de objeto múltiple reguladas, sociedades financieras populares, instituciones para el depósito de valores, contrapartes centrales, instituciones calificadoras de valores, sociedades de información crediticia, sociedades financieras comunitarias, sujetas a la supervisión de la Comisión y los organismos de integración financiera rural, así como otras instituciones y fideicomisos públicos que realicen actividades financieras y respecto de los cuales la Comisión ejerza facultades de supervisión, todas ellas constituidas conforme a las leyes mercantiles y financieras. Entran también las instituciones financieras del exterior o sociedad controladora filial.

> *...a raíz de la firma del Tratado trilateral de Libre Comercio para la América del Norte, fueron reformándose nuestros ordenamientos jurídicos para permitir el establecimiento y operaciones de empresas extranjeras dentro del sector financiero nacional, los cuales quedaban sujetos inicialmente a condiciones de participación gradual dentro de nuestro mercado.*[102]

Para el verbo rector *modificar,* es hacer una cosa diferente de como era antes, alterar, enmendar, reformar o transformar una cosa alterando sus características; mientras que *destruir*, es reducir a pedazos o a cenizas algo material, u ocasionarle un grave daño, deshacer o inutilizar algo.

La expresión *causar la pérdida*, se desprende de la doctrinal y se entiende como producir cierto efecto o dar lugar a cierta consecuencia que en este caso es la pérdida irreparable de la información o datos contenidos dentro del sistema o equipo informático.

[102] Carvallo Yáñez, Erick, Nuevo derecho bancario y bursátil mexicano, Teoría y práctica de las agrupaciones financieras, las instituciones de crédito y las casa de bolsa, Editorial Porrúa, novena edición, México, 2014, p.33.

ELEMENTOS SUBJETIVOS

El elemento subjetivo genérico consistente en el dolo en su modalidad de dolo directo, de tal suerte que se presentan en la psique del sujeto activo, tanto el elemento cognoscitivo al conocer de los elementos del tipo penal, como el elemento volitivo al querer el resultado típico de modificar, destruir o causar la pérdida de la información ya sea en sistemas o en equipos de informática propiedad de las entidades financieras integrantes del Sistema Financiero Mexicano.

Para finalizar, y a manera e resumen del presente capítulo donde se analizó los elementos de los tipo penal concerniente a cada uno de los denominados acceso ilícito a sistemas y equipos de informática, elementos como: la acción, el bien jurídico tutelado, la forma de participación del sujeto activo, las calidades específicas tanto del sujeto activo como del pasivo, el objeto material, los medios comisivos, las circunstancias de tiempo, modo, lugar y ocasión, los elementos normativos y el carácter doloso de la conducta. De tal suerte que lo desarrollado hasta aquí demuestra la importancia de conocer a profundidad cada elemento de la clasificación jurídica para su debida acreditación, no obstante al reducido campo de acción de la legislación penal mexicana con respecto a los sistemas informáticos.

Así mismo, es evidente que falta mucho por legislar pues las conductas ilícitas que se cometen a través de los sistemas de telecomunicaciones como el internet, sobrepasan a las que se perpetran mediante el simple acceso sin autorización a un sistema o equipo de informática. Como se describió en el capítulo tercero, no es necesario ingresar a los sistemas informáticos para menoscabar o lesionar el bien jurídico tutelado, basta con enviar programas informáticos conocidos como malware para provocar daños irreparables a dichos sistemas.

CAPÍTULO QUINTO

PROPUESTA DE PERSECUCIÓN DE LOS DELITOS INFORMÁTICOS

La propuesta que quiero desarrollar en este capítulo con relación a la persecución de los delitos informáticos gira en torno de dos vertientes, por un lado, lo relacionado con la tipificación de los delitos que no están considerados en el Código Penal Federal, para que de esta manera, puedan ser perseguidas las personas que incurran en ellos, de lo contrario se estaría violando el principio de legalidad enmarcado en el artículo 14 constitucional en su párrafo tercero; por otro lado, la forma de cómo se debe llevar a cabo la investigación científica de los mismos, detallando la técnica del rastreo de una terminal que haya sido el medio comisivo de un delito informático.

El tema de la investigación forense cobra principal protagonismo en este siglo, y la necesidad de una preparación interdisciplinaria es por demás relevante, como lo sugiere Don Jacobs, "*un currículum interdisciplinario basado en la ciencia y la tecnología con un cimiento académico sin fisuras*",[103] entonces la ciencia del derecho de ninguna manera debe ser ajena a las otras ciencias, sobre todo cuando se ha tratado en esta tesis de los importantes avances en materia de telecomunicaciones que se han generado en el mundo.

Este capítulo contiene de manera específica las propuestas técnicas y legales que, desde mi experiencia como Ingeniero y Licenciado en Derecho, México debe considerar si es que en verdad queremos acortar esa brecha de décadas que tenemos de rezago tecnológico en la persecución de delitos.

[103] Jacobs, Don, *Analyzing Criminalminds, Forensic Investigative Science for the 21st Century*, Brain and Evolution Patrick McNmara, Series Editor Praeger. USA 2011, p.8. "*college students a science-based and technology rich interdisciplinary curricula with seamless academic transfer leading to bachelor ' s, master ' s, and doctoral degrees in university studies. It is my hope that students receive 21st-century training through interdisciplinary forensic investigative sciences*"

5.1 La Investigación

De conformidad con el CNPP en su artículo 211, la investigación se conforma de dos fases:

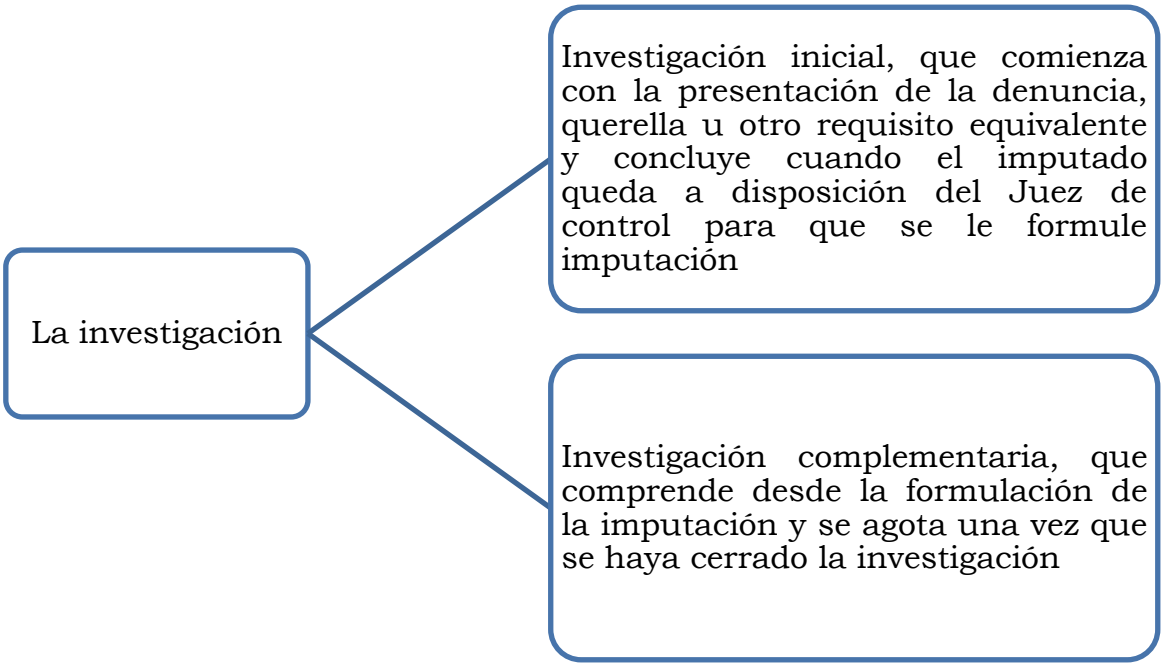

Figura 5.1. La investigación conforme al CNPP.

La investigación de los delitos corresponde a la llamada trilogía de la investigación conformada por las policías y los peritos, que actuarán bajo la dirección estratégica del Ministerio Público (MP). La misma legislación penal sugiere que la investigación tiene las siguientes características i) inmediata, ii) eficiente, iii) exhaustiva, iv) profesional, y v) orientada a explorar todas las líneas de investigación posibles que permitan el esclarecimiento del delito. Esta etapa se desarrolla en una fase de investigación desformalizada, seguida de una fase de investigación formalizada. En la primera, el MP debiendo recabar aquellos datos de prueba pertinentes, idóneos y en su conjunto suficientes que sustenten su ejercicio de la acción punitiva, apreciará los actos de detención de una persona, la interposición de la denuncia o la querella, la realización de diligencias de

investigación y la recolección de datos de prueba; contando para todo ello con la colaboración de los cuerpos de seguridad pública y con el Instituto de Servicios Periciales de la Procuraduría; observando en todo momento los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez, lealtad y respeto de los derechos humanos.

El Ministerio Público solicitará la información a toda persona o servidor público quienes estarán obligados a proporcionar oportunamente la misma y si son requeridos para ser entrevistados, también la ley los obliga para comparecer y sólo podrán excusarse de manera excepcional. Durante la investigación, el MP ordenará que se lleven a cabo todos aquellos actos de investigación que sean conducentes, considerados pertinentes y útiles para el esclarecimiento de los hechos. Toda la información, así como las actuaciones deberán ser registradas, utilizando al efecto cualquier medio que permita garantizar que la información recabada sea completa, íntegra y exacta, para que de esta forma el acceso a la misma por la parte interesada goce de un grado de certeza.

La investigación inicia cuando el MP tiene conocimiento de la probable comisión de un hecho delictivo cuya persecución dependa de querella o de cualquier otro requisito equivalente; éste iniciará la investigación conforme a las técnicas previstas en el CNPP, como la cadena de custodia, la cual consiste en control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización, descubrimiento o aportación, en el lugar de los hechos o del hallazgo; se aplicará teniendo en cuenta la identidad, el estado original, las condiciones de recolección, la preservación, el empaque y el traslado; lugares, fechas y cambios que en cada custodia se hayan realizado, registrando el nombre y la identificación de todas las personas que hayan estado en contacto con esos elementos. Lo anterior con el objeto de que los indicios, huellas o vestigios del hecho delictivo, así como los instrumentos, objetos o productos del delito no se alteren y no pierdan su valor probatorio.

Una vez practicadas las diligencias investigativas estimadas útiles y pertinentes para esclarecer el hecho, el MP deberá analizar los elementos de juicio

colectados, con el objeto de alcanzar un estado de convicción que le permita definir qué trámite conviene en el caso.

Finalmente, y como refiere Robin Bryant, "*investigar la delincuencia digital no significa por sí mismo que se lleve a cabo una investigación forense digital. Algunos crímenes digitales, como el fraude de identidad donde el sospechoso utiliza Internet como fuente de información y como medio para cometer el delito, podrían ser técnicas de investigación forense de internet. Sin embargo, muchos crímenes digitales también requieren una forma especializada y paralela de investigación forense digital*".[104]

De manera concreta la figura 5.2, ilustra algunas componentes de la investigación digital forense; sin embargo, no significa que todos serán usados en una investigación en particular, así para un análisis de *email* se podrá utilizar tanto el análisis de red y del servidor (network and server forensics), como la informática forense (Computer forensics).

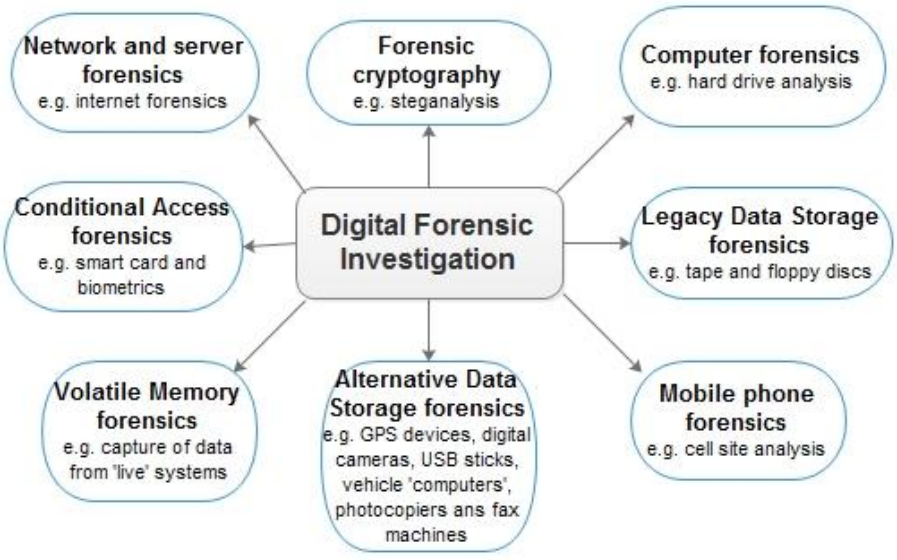

Figura 5.2. Campos de especialidad dentro de la investigación digital[105]

[104] Bryant Robin, op. cit. nota 26, p. 70
[105] Ídem

5.2. Informática Forense

La Informática Forense se entiende como una disciplina auxiliar de las ciencias forenses, que por su carácter científico y sus fundamentos en las leyes de la física como la electricidad, magnetismo y cuántica, maneja e interpreta la información que se almacena en medios con ésta naturaleza; apoyándose en el método científico aplicado a la recolección, análisis y validación de todo tipo de pruebas, permite establecer los hechos y formular las hipótesis relacionadas con la ciberdelincuencia.

> *A la fecha, existen múltiples definiciones sobre el tema forense en informática. Una primera revisión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, digital forensics, network forensics, entre otros. Este conjunto de términos puede generar confusión en los diferentes ambientes o escenarios donde se utilice, pues cada uno de ellos trata de manera particular o general temas que son de interés para las ciencias forenses aplicadas en medios informáticos.*[106]

Existen distintas fases y modalidades de actuación relacionadas con la informática forense que, a lo largo de un proceso penal, llevan a cabo expertos, investigadores y profesionales del derecho; por ejemplo, la planificación previa, la identificación, recolección, validación, análisis, interpretación, documentación y presentación de la evidencia digital para ayudar a esclarecer y/o probar sucesos de naturaleza delictiva. [107]

Con el desarrollo de esta disciplina se ha trabajado sobre su principal objeto de estudio, que es *la evidencia digital*. El término evidencia se suele asociar con elementos físicos, que se pueden captar con los sentidos, es así que al mencionar *evidencia*, naturalmente hace referencia a la *evidencia física*. Esto pareciera ser contrastante con el término *evidencia digital*, por cuanto, todo aquello relacionado con el término *digital* se ha asimilado al término *virtual*, es decir, como no real. Es

[106] J. Cano M., Jeimy, *Computación Forense, descubriendo los rastros informáticos*, 2a Ed. Editorial Alfaomega, México, 2015, p.19

[107] Haydée Di Iorio, Ana, et al, *El rastro digital del delito, aspectos técnicos, legales y estratégicos de la Informática Forense*. GRUPO DE INVESTIGACIÓN EN SISTEMAS OPERATIVOS E INFORMÁTICA FORENSE, Universidad FASTA, 2016.

de importancia destacar que los datos o evidencia digital siempre están almacenados en un soporte real, siendo este último de tipo físico, por lo que esta clase de evidencia podría considerarse igualmente física.

> *Desde el advenimiento del microprocesador, de los dispositivos de almacenaje asequibles, y de las redes, más de nuestras vidas diarias se están registrando en los unos y ceros del mundo digital. Por lo tanto, no es de extrañar que cuando se cometan crímenes y delitos, a menudo hay evidencia de valor probatorio almacenado o transmitido en forma digital. De hecho, esta es la definición de la evidencia digital (DE) según el Grupo de Trabajo Científico sobre Evidencias Digitales (SWGDE. Scientific Working Group on Digital Evidence)*[108]

MANEJO DE CASOS FORENSES DIGITALES

Actualmente se utiliza un proceso bien definido de cuatro etapas que se aplican en casos forenses digitales, sin importar la evidencia o circunstancias y está definido en la siguiente figura 5.3.

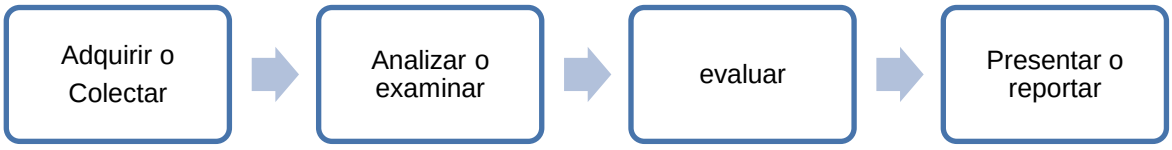

Figura 5.3. Proceso Forense Digital[109]

Registrar en sitio la escena física y duplicar la evidencia digital mediante procedimientos forenses estandarizados y aceptados internacionalmente; así

[108] Mozayani, Ashraf and Noziglia, Carla, *The forensic laboratory handbook: procedures and practice*. Steven B. Karch, MD, Series Editor, Humana Press Inc. New Jersey. 2006, p.79

[109] Watson, David and Jones, Andrew, *Processing and Procedures, Meeting the Requirements of ISO 17020, 17025, 27001*. Editorial Project Manager: Heather Scherer, USA 2013, p. 369. No obstante que existen otros modelos de investigación digital como el Cassey 2004, el DFRWS 2001, NIJ 2001, NIJ 2004 y el Cohen 2009, este último sugiere las siguientes etapas: Identify, Collection, Preserve, Transport, Store, Analyze, interpret, Attrybute, Reconstruct, Present and Destroy. Casey, Eoghan, *Digital evidence and computer crime, Forensic science, computers and the internet*, Third Edition, Elsevier, USA, 2011, p. 189.

como, examinar en profundidad y una búsqueda sistemática de pruebas relativas al incidente sospechoso; esto se centra en la identificación y localización de pruebas potenciales, posiblemente en lugares no convencionales o encubiertos como se define en la sección de *adquirir o colectar*.

El Análisis para determinar significados, reconstruir fragmentos de datos y sacar conclusiones basadas en la evidencia encontrada; puede tomar varias iteracciones de examen y análisis para apoyar los resultados.

Evaluación que determina la relevancia de la evidencia recuperada, típicamente realizada por los abogados involucrados. No sólo se evaluará el contenido de las pruebas, sino también la cadena de custodia en esta etapa.

Además, la presentación al resumir y proporcionar explicación de las conclusiones, esto debe escribirse en términos claros evitando el uso de terminología abstracta.

Adicionalmente, la Asociación Internacional Especialista en Investigación Informática (*IACIS por sus siglas en inglés The international Association of Computer Investigative Specialist*)[110] que es actualmente una organización internacional especializada en la formación y certificación en el campo de la informática forense, ha declarado que existen tres requisitos esenciales para la realización de un examen de forense digital competitivo:

- Se deben utilizar soportes de examen estériles forenses.
- El examen debe procurar la integridad de los medios originales.
- Las copias impresas, las copias de los datos y las pruebas resultantes del examen deben estar debidamente marcadas, controladas y transmitidas

En resumidas cuentas, la herramienta a utilizar para el manejo y almacenamiento de la información digital debe estar por duplicado, esto es, contener una imagen del disco o partición original, no debe alterar la original y estar libre de errores, contener información correcta procurando que la unidad de almacenamiento sea

[110] Información consultada en septiembre de 2017 en la siguiente liga: https://www.iacis.com/

de mayor capacidad a los datos copiados, pues un informático forense no trabaja con el soporte original, sino con una imagen a bajo nivel adquirida a partir del mismo.

> *Para adquirir un soporte es necesario establecer una conexión hardware. El método habitual consiste en desmontar el disco duro, llevarlo al laboratorio y conectarlo a una estación de trabajo forense. Si se trata de un disco IDE se puede conectar en el primer interfaz IDE como Máster o Slave (dando por supuesto que en el Máster está el disco con el sistema operativo y las herramientas de investigación forense) o en el segundo interfaz IDE como Máster o Slave, dependiendo de lo que tangamos instalado -grabadora dvd o disco duro de gran capacidad para almacenar la imagen-; si el disco es de tipo SATA se podrá conectar a cualquiera de los interfaces SATA que tengamos disponibles.*[111]

Para facilitar el análisis del soporte de datos se puede seguir una metodología similar al modelo OSI de las redes, donde como ya sabemos el nivel uno corresponde a la capa física y es aquí donde tienen cabida los discos duros, USB, chips de teléfonos móviles y *smartphones*.

El nivel dos correspondería a los volúmenes y particiones de los discos duros. Es decir, hablamos de un disco duro dividido en bloques de datos básicos o sectores, en pistas o grupos de sectores que hacen un giro completo en el plato y en cilindros como el conjunto de pistas situadas en la misma posición de todos los platos. Así, una partición consiste en un grupo de cilindros contiguos; por el contrario, el volumen no tiene por qué ser contiguo, pudiendo estar compuesto por varias particiones situadas a lo largo del disco duro.

Con respecto al nivel tres, éste puede ser representado por el sistema de archivos, el cual determina la referencia exacta de los sectores que ocupan el contenido de cierto archivo de texto, imagen o sonido, estructurándolas en tablas para que el

[111] Lázaro Domínguez, Francisco, *Introducción a la Informática forense*, RA-MA Editorial, Madrid, 2012, p.48.
La interfaz ATA, P-ATA o PATA, originalmente conocida como IDE, es un estándar de interfaces para la conexión de dispositivos de almacenamiento masivo de datos y unidades de discos ópticos que utiliza el estándar derivado de ATA y el estándar ATAPI.Los términos IDE (Integrated device Electronics), EIDE (Enhanced IDE) y ATA, hoy en día PATA, se han usado como sinónimos ya que generalmente eran compatibles entre sí.Por otro lado, aunque hasta el 2003 se utilizó el término "ATA", con la introducción del Serial ATA (SATA) se le acuñó el retrónimo Parallel ATA (PATA).

sistema operativo tenga acceso. Dentro de los más comunes están NTFS, FAT, EXT, HFS, etc.

El nivel cuatro contempla los bloques de datos o *cluster*, la cual representa la unidad de menor tamaño disponible para el almacenamiento de datos en una partición, usualmente de 512 bytes de longitud. Si el bloque está asignado a un archivo gráfico, contendrá información codificada JPEG, PNG. Si se trata de un documento XML o DOC.

El nivel cinco corresponde a los Metadatos, que se definen como datos que hacen referencia a otros datos. Por lo general este nivel ofrece al investigador marcas de tiempo en la creación, acceso, modificación; de identidad del propietario del archivo y punteros a los bloques de datos en los que se encuentran almacenado el contenido.

El nivel seis se relaciona con el nombre de archivo, es la interfaz humana del sistema de archivos, compuesta por nombres que definen el contenido. Compuesto por nombres de archivos y directorios, los cuales incluyen punteros a las estructuras de metadatos correspondientes.

Finalmente, el nivel siete correspondería al conjunto de características para verificar que todas las operaciones de actualización de los metadatos y otras estructuras de control del sistema de archivos se lleven a cabo. A este sistema de registro de transacciones se le conoce como *journaling*.

A manera de ejemplo casero, podemos ver cómo está particionado el disco duro 0 y las memorias USB Disco 1 y 2 respectivamente, para este caso se trata de una NOTEBOOK marca Ienovo particionado en unidad (C:) y (D:) con un sistema de archivo NTFS porque el sistema operativo es Windows 7, la herramienta que proporciona Microsoft es *Administración de Equipos*, la cual se puede abrir siguiendo la ruta: Inicio_Panel de Control_Sistemas y Seguridad_Herramientas administativas_ Administración de Equipos. Ver figura 5.4.

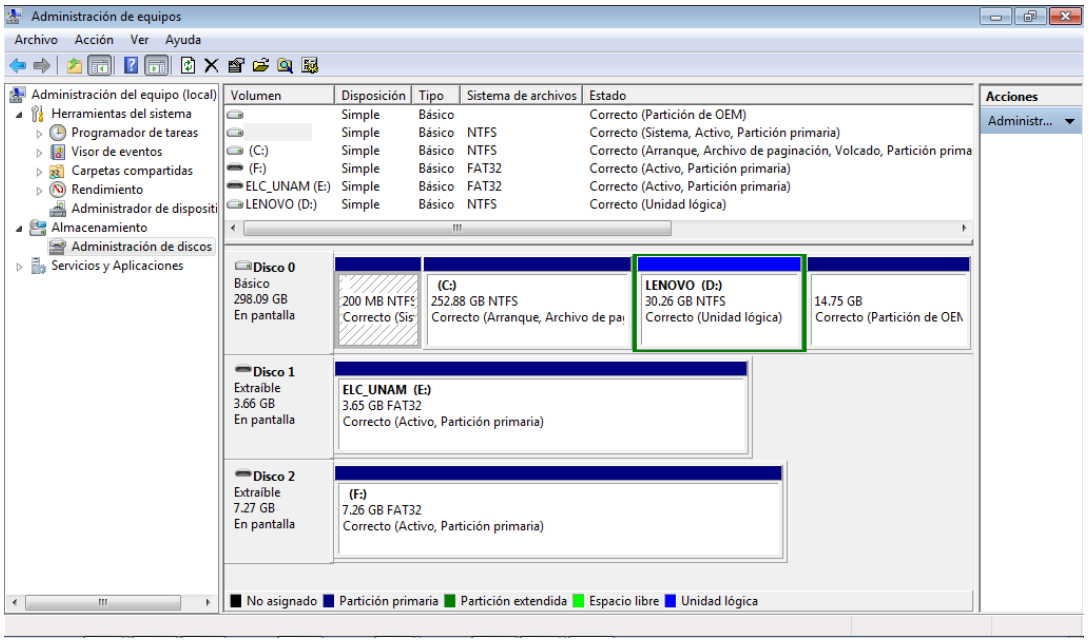

Figura 5.4 Partición de disco duro en Windows 7.

5.3 Transferencia de datos

Para poder investigar aplicando la informática forense sobre los casos de *network and server forensics* como *volatile memory forensics*, considero necesario conocer los elementos básicos de un sistema de comunicación en su nomenclatura más básica; estructurada con un emisor, un mensaje, un medio de transmisión y un receptor, donde el emisor es el sujeto que envía la información, además es quien prepara la información para enviarla al receptor, quien a su vez recibe esa información al recuperar de nuevo el mensaje; el medio de transmisión es el canal a través del cual viaja el mensaje. No obstante su simplicidad, una comunicación a través de una red de datos proporciona un cúmulo de evidencias para ser analizadas entre las que encontramos archivos en un medio de almacenamiento electrónico, líneas de texto *logs* de transacciones, registros de acceso a sitios web, datos en el registro de auditoría de aplicaciones, datos de una ocurrencia en los registros de eventos del sistema, etcétera.

Además, es necesario traer a tema en la tesis, los principios de la criminalística que a mi juicio son aplicables en el ámbito de la delincuencia informática y que a la postre serán la base de la propuesta de persecución, por ejemplo el Principio de Transferencia, el cual postula que: "*es imposible que un delincuente actúe, bajo la tensión de la acción delictiva, sin dejar rastros de su presencia*",[112] estos rastros de evidencias lo constituyen los registros de transferencias de paquetes almacenados como datos en los históricos de eventos de la misma computadora. Otro principio que vale la pena recordar es el de Reconstrucción de los Hechos, que en realidad es el propósito de la labor investigativa y probatoria; en la búsqueda, obtención y análisis de evidencias ha de contribuir al conocimiento o reconstrucción de esos hechos pasados, los registros almacenados de manera secuencial evidencian lo ocurrido. Un tercer Principio importante también lo es el de Certeza, el cual se trata del estudio cuantitativo, cualitativo y comparativo de las evidencias, para determinar su procedencia, su contenido y su finalidad; todo para establecer si la evidencia se encuentra vinculado con los hechos delictivos.

Abordando un poco más sobre la transferencia de los datos a través de un sistema informático, conviene recordar que las redes están integradas por diversos componentes que trabajan juntos para crear un sistema, estos componentes están estandarizados para su interconexión entre sí, de tal suerte que con ello se logre establecer la comunicación; los tres estándares a que me refiero y que son los más populares y se utilizan en la actualidad son: Ethernet, ARCnet y Token Ring.

Ethernet y Token Ring son estándares respaldados por IEEE (Instituto de Ingenieros Eléctricos y Electrónicos por sus siglas en inglés); ARCnet es un estándar de ANSI (Instituto Nacional de Estándar Americano, por sus siglas en inglés). Sólo para ejemplificar en este trabajo de tesis explicaré de una forma sencilla como funciona Ethernet; donde las velocidades de envío de paquetes que utilizan la tecnología Ethernet son de 10 Mbps (Ethernet estándar), 100 Mbps (Fast Ethernet – 100BASEX) y de 1000 Mbps utilizando el Giga bit Ethernet. Las redes Ethernet tienen un esquema de direccionamiento de 48 bits. A cada

[112] Ibídem, p. 54

computadora conectada a una red Ethernet se le asigna un número único de 48 bits conocido como dirección Ethernet (Dirección fuente o Dirección destino).

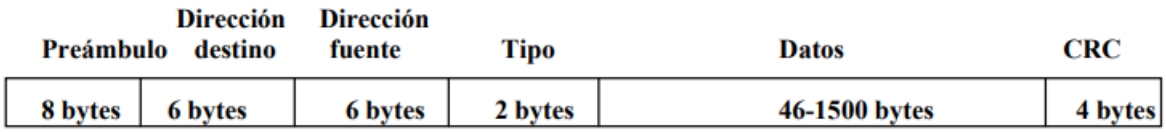

Figura 5.5 Formato de una trama Ethernet.

La trama de Ethernet es de una longitud variable pero no es menor a 64 bytes ni rebasa los 1518 bytes (Encabezado (que comprende: preámbulo, dirección destino, dirección fuente y tipo), Datos y CRC), cada trama contiene un campo con la información de la dirección de destino. En la figura 5.5 se muestra una trama Ethernet. La mayor ventaja de que las tramas se auto-identifiquen es que éstas permiten que múltiples protocolos se utilicen juntos en una sola máquina y sea posible entremezclar diferentes protocolos en una sola red física sin interferencia. Teniendo estos elementos básicos de transmisión, es momento que abordemos el principio de *encapsulamiento*; porque las aplicaciones que se desarrollan con TCP/IP, normalmente utilizan un conjunto de protocolos para llevar a cabo la comunicación. La suma de las capas de este conjunto de protocolos se conoce como stack de protocolo. De esta forma, cuando una aplicación envía datos usando el protocolo TCP, el dato es enviado hacia abajo del protocolo stack a través de cada capa del modelo OSI, hasta que este se envíe como un flujo de bits a través de la red. Cada capa coloca información adicional al dato en su encabezado para que éste sea recibido. En la figura 1.4 del primer capítulo, se muestra este proceso. Los números abajo de los encabezados y del CRC (Chequeo Cíclico de Errores, por sus siglas en inglés) conforman la trama Ethernet y representan los tamaños típicos en bytes. Una propiedad física de una trama Ethernet es que la MTU (Unidad Máxima de Transmisión) por default es del tamaño de 1500 bytes.

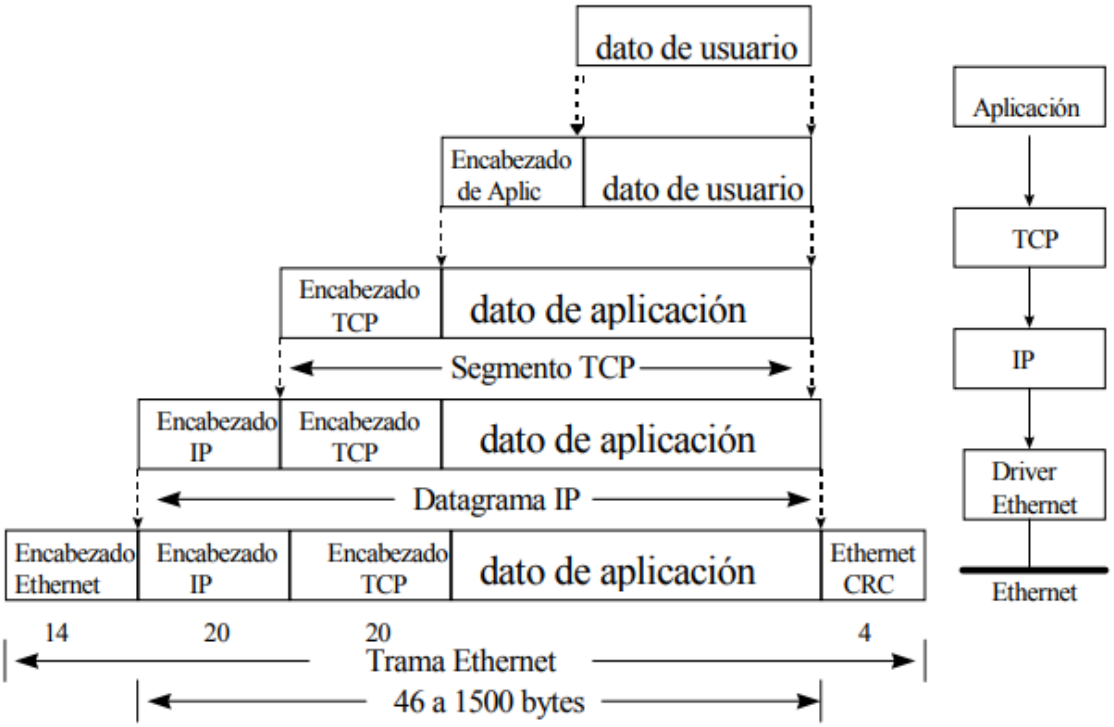

Figura 5.6. Encapsulado de un dato.

El proceso que utiliza una aplicación para transferir el contenido de un archivo se muestra en la figura 5.6, y es el siguiente:

1. La capa de la aplicación envía un flujo de bytes a la capa de transporte de la computadora de origen.

2. La capa de transporte divide el flujo en segmentos TCP, asigna un encabezado con un número de secuencia al segmento y transmite este segmento a la capa de Internet IP, y se calcula la suma de comprobación.

3. La capa de IP crea un paquete con parte de los datos que contiene el segmento TCP. La capa de IP añade al paquete un encabezado que indica las direcciones IP de origen y de destino. Esta capa también determina la dirección física de la computadora destino o las computadoras que actúan como intermediarios hasta el host destino. Entonces, envía el paquete y la dirección física a la capa de enlace de datos y se vuelve a calcular la suma de comprobación.

4. La capa de enlace de datos transmite el paquete IP en la sección de datos de una trama de enlace de datos a la computadora destino. Si la computadora destino actúa como intermediario, el paso 3 volverá a repetirse hasta que se alcance el destino final.

5. Cuando se alcanza la computadora destino, la capa de enlace de datos

descarta el encabezado del enlace y envía el paquete IP a la capa de IP.

6. La capa de IP verifica el encabezado del paquete. Si la suma de comprobación del encabezado no coincide con la calculada por dicha capa, el paquete se ignora.

7. Si las sumas coinciden, la capa IP descarta el encabezado y envía el segmento TCP a la capa TCP correspondiente. Esta capa comprueba el número de secuencia para determinar si el segmento, es el segmento correcto de la secuencia.

8. La capa TCP calcula una suma de comprobación para los datos y el encabezado TCP. Si la suma no coincide con la suma transmitida con el encabezado, la capa TCP descarta el segmento. Si la suma coincide y el segmento está en la secuencia correcta, la capa TCP envía un reconocimiento a la computadora destino.

9. La capa TCP descarta el encabezado TCP y transfiere los bytes del segmento que acaba de recibir a la aplicación.

10. La aplicación que se encuentra en la computadora destino recibe un flujo de bytes como si estuviera conectado directamente a la aplicación de la computadora origen.

Como se puede observar, la forma en que se interconectan dos computadoras es mediante paquetes de datos establecidos por protocolos de comunicación bien definidos estructuralmente, pues se requiere precisar dónde empieza la información toda vez que, lo que se transmite no son más que cadenas de bits o caracteres conformados de unos y ceros; así mismo no hay que olvidar que "*la necesidad clara de construir un sistema interconectado mundial entre todas estas redes fue uno de los motores fundamentales de Internet*"[113]. Es decir, la construcción de una red de redes.

Internet conquistó el mundo a través de dos tecnologías clave como el protocolo Internet (IP), que permite conectar a Internet a cualquier tecnología de red existente. De esta manera Internet provee básicamente la funcionalidad que permite que cualquier computadora conectada a esta red pueda conectarse a un servidor identificado por una dirección IP.

[113] Gutiérrez Gallardo, Claudio, Cómo funciona la Web, Centro de Investigación de la Web Departamento de Ciencias de la Computación Universidad de Chile, 2008, p.44

Finalmente en el ámbito de Internet, un puerto es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host, o puesto de trabajo. Muchos de los puertos se asignan de manera arbitraria, pero hay algunos que se asignan, por convenio, a ciertas aplicaciones particulares o servicios de carácter universal. De hecho, la IANA (*Internet Assigned Numbers Authority*)[114] determina las asignaciones de todos los puertos comprendidos entre los valores [0, 1023]. Por ejemplo, el servicio de conexión remota telnet, usado en Internet se asocia al puerto 23, el puerto de datos FTP es el 20, 25 para SMTP, HTTP tiene el 80, etc.[115]

5.4 Rastreo de evidencia con Wireshark

Como se abordó en el capítulo tercero, *de los delitos informáticos*, ahí nos percatamos que existen diferentes y variadas conductas que representan los tipos penales informáticos; asimismo, se tiene que existen diferentes casos donde se emplea la investigación forense, como también se ha mencionado en el presente capítulo (para mayor referencia ver figura 5.1.), Ahora, dentro de los casos más comunes se encuentran:

- El inapropiado uso de un sistema de procesamiento informático.
- El acceso sin autorización
- El ataque de malware en cualquier variante

Con respecto a la recopilación de pruebas o evidencia, cuando la conducta se relaciona con el acceso sin autorización de un equipo o sistema informático, depende en gran medida del caso en específico; no obstante, podemos hablar de las siguientes cinco acciones para su ejecución:

[114] https://www.iana.org/ Responsable de coordinar algunos de los elementos clave que mantienen Internet funcionando sin problemas. Aunque Internet es reconocida por ser una red mundial libre de coordinación central, existe una necesidad técnica de coordinar globalmente algunas partes clave. Consulta Octubre de 2017.

[115] http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html. En esta página se pueden ver la asignación de los puertos lógicos de comunicación más comunes usados por servicios, dominios y programas designados por IANA. Consulta Octubre de 2017.

a) Escanear el sistema atacado y de ser posible el sistema del atacante, para determinar los hechos.
b) Utilizar en la medida de lo posible, las bases de datos de incidentes para ver si otras personas han sufrido ataques similares y lo que hicieron.
c) Usar inteligencia de fuente externa sobre el atacante; cualquier hecho conocido sobre él.
d) Validar la dirección IP del atacante. Hay que tener cuidado de que los atacantes no sean alertados. Nunca se debe utilizar una dirección IP rastreable. El atacante puede haber utilizado una dirección dinámica.
e) Utilice evidencia en sitio para identificar a los atacantes (v. gr., registros de acceso(logs) e imágenes de CCTV)

Ahora bien, el uso de la herramienta idónea para el análisis de evidencia digital es indispensable, aplicaciones que existen en el mundo informático tales como Wireshark, el cual es un analizador de protocolos que funciona sobre los sistemas operativos de Windows y Unix, su principal objetivo es el análisis de tráfico; con esta aplicación se pueden visualizar los campos de cada una de los encabezados y capas que componen los paquetes monitoreados; incluye una versión en línea de comandos y una versión gráfica.[116]

La forma más común para conectar el analizador se muestra en la siguiente figura 5.7, donde se observa la computadora con la aplicación wireshark, el servidor que será analizado y un dispositivo de interconexión conocido como hub, que sirve de enlace con la red de datos ejemplificada aquí a través del switch. Todo el tráfico entre el switch y el servidor podrá analizarse con la aplicación wireshark.

[116] Borja Merino Febrero, *Análisis De Tráfico Con Wireshark*, Instituto Nacional de Tecnología de la Comunicación, Febrero, 2011. Consulta 9 de Agosto 2017 20:30 horas. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

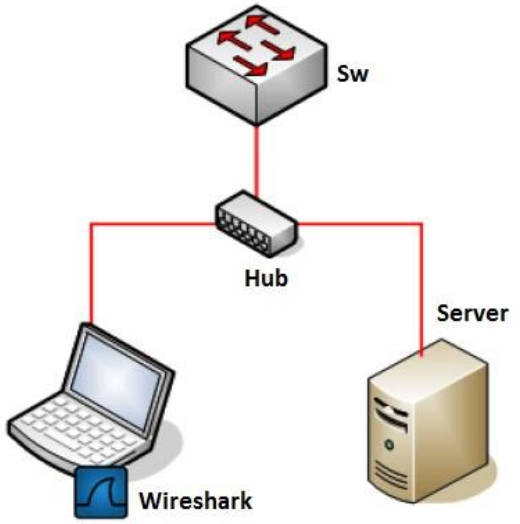

Figura 5.7. Conexión de Wireshark[117]

Wireshark es un software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android, y Mac OS X, así como en Microsoft Windows.

Como puede verse en la figura 5.8, la interfaz gráfica de la aplicación Wireshark se conforma de 4 campos o áreas de trabajo, de arriba hacia abajo está la primera área de trabajo que es el de filtrado (filter), la cual permite definir patrones de búsqueda para visualizar aquellos paquetes o protocolos que se quieran rastrear.

La segunda área corresponde a la lista de todos los paquetes que se están capturando en línea, se visualizan los datos como: tipo de protocolo, números de secuencia, flags, marcas de tiempo, puertos, etcétera (zona color verde).

[117] Ibídem p.9

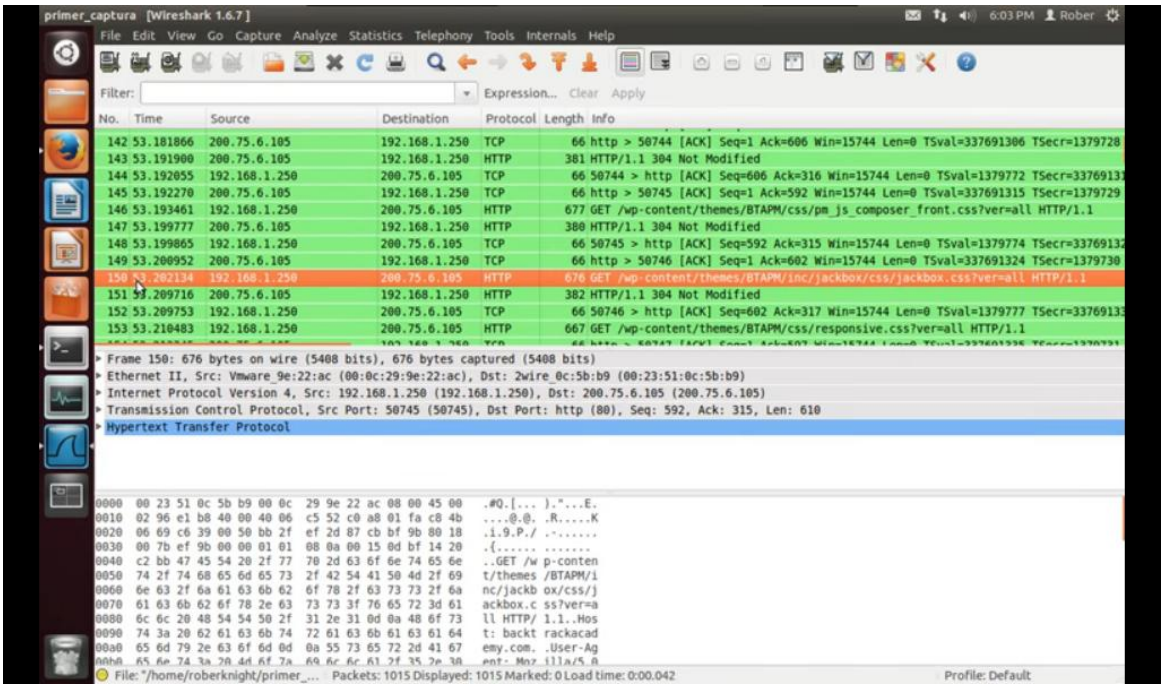

Figura 5.8 Interfaz Gráfica de Wireshark.

La tercera área (gris) permite desglosar por campos cada una de los encabezados de los paquetes seleccionados en el área 2 (v.gr., la trama No. 150 tiene una longitud de 676 bytes, IP versión 4 y se utiliza el protocolo TCP para la aplicación http: Hypertext Transfer Protocol).

Finalmente la cuarta área representa, en formato hexadecimal del paquete, es decir, tal y como fue capturado por la tarjeta de red. Sólo basta señalar que el formato hexadecimal es un sistema de numeración posicional que tiene como base el 16 (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E y F); v.gr., el *6B* hexadecimal equivale al 107 en decimal o en binario al “0110 1011”.

Cuando existe una gran cantidad de tráfico ARP que se está recibiendo, esto se refleja en la segunda área de la aplicación, y sí se observa más detalladamente este comportamiento del protocolo, es una clara muestra de que el servidor está siendo víctima de un ataque. En la figura x, se observan sólo paquetes TCP y HTTP. Existen multitud de herramientas gratuitas destinadas a detectar este tipo

de ataques, v.gr. Arpwatch, Nast, Snort, Patriot NG, ArpON, entre otras, que permiten generar alertas cuando se detecta un uso anormal del protocolo ARP.

Así mismo, no sólo el tráfico ARP es sinónimo de ataque, ya que un tipo de ataque DoS son los conocidos ataques "*Smurf"* donde se envían paquetes ICMP a una dirección "*broadcast"* con una IP origen falsificada; dicha IP falsificada será el objetivo del ataque al recibir múltiples paquetes de respuesta "*echo reply"* (contestación) como consecuencia del paquete "*broadcast"* enviado por el atacante.

Wireshark también soporta otros tipos de servicios como los de geolocalización de MaxMind, figura 5.9; con los cuales se pueden obtener ciudades y países asociadas a las IPs capturadas proporcionando información sobre la procedencia de los paquetes. En determinados escenarios en los que somos víctimas de un DDoS o en el caso de Botnets podría ser de gran ayuda conocer el origen de los mismos de forma visual. V.g. GeoIP, GeoLiteCity y GeoIPASNum.

Además del rastreo de información a través de las IPs, también existen técnicas o métodos que se realizan utilizando direcciones MAC, pues ésta actúa como identificador único de una tarjeta de red asignada a cada computadora a nivel mundial, y como se trató en el primer capítulo, ésta se utiliza en la subcapa del protocolo de control de acceso del modelo de referencia OSI.

Finalmente, la realización de un reporte del caso permite manejar y entender la situación en análisis; además muestra la evidencia encontrada y cómo ésta soporta o no los requerimientos de un cliente en específico. Por lo anterior en la tabla 5.1, anexo mi propuesta de los contenidos básicos que debe contener un informe de informática forense.

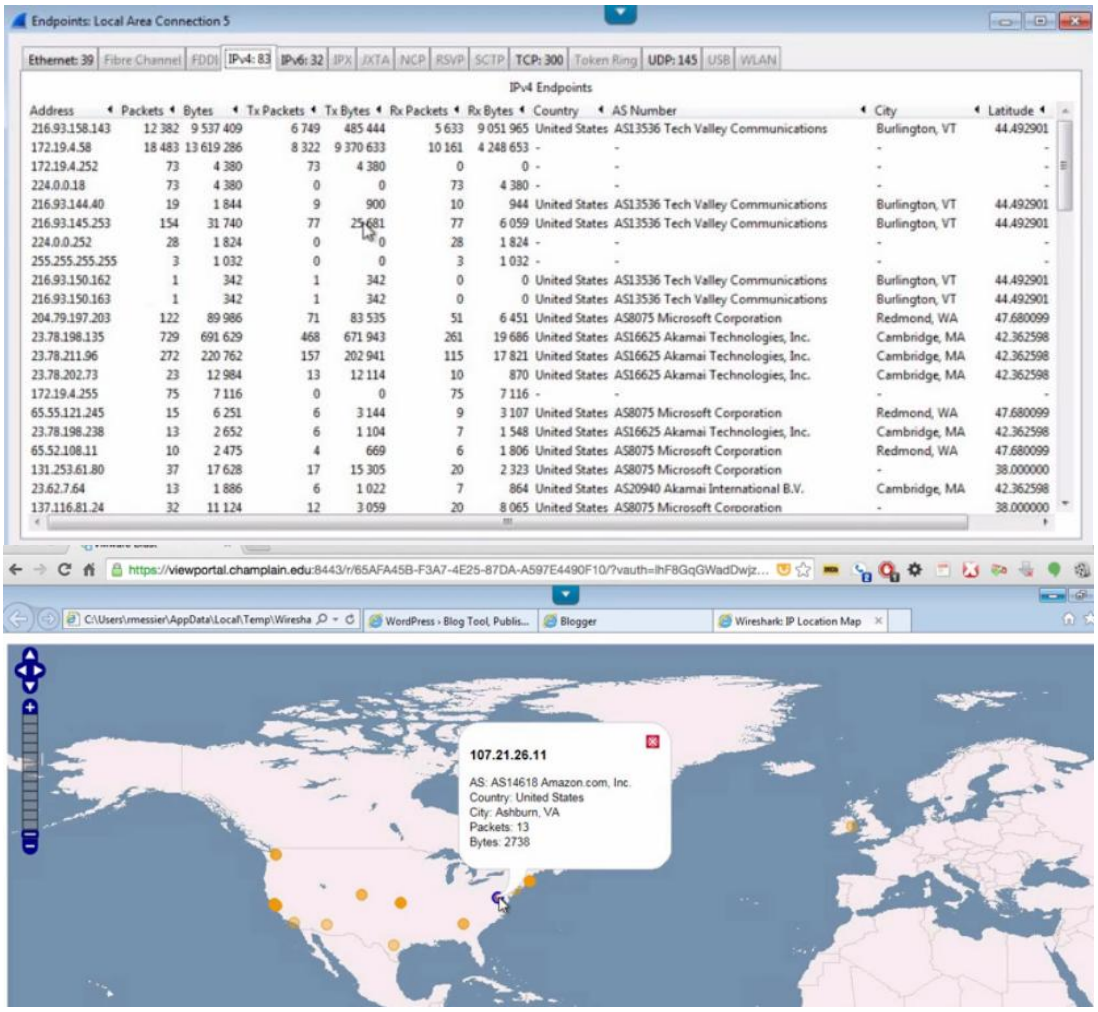

Figura 5.9. Interfaz de geolocalización de Wireshark.

Informe Forense			
Nombre:	**Cliente:**	**Asunto:**	
Control de documentos	**Pruebas requeridas por el cliente:**		**Conclusiones:**
			Sugerencias:
	Resultados de la investigación:		
Pruebas encontradas hasta la fecha:			
			Firma:

Tabla 5.1. Propuesta de plantilla para un Informe de informática forense.

5.5 Derecho comparado

La función del derecho comparado es parecido al de la historia, dándole al estudioso del derecho nacional la perspectiva necesaria para tener una visión adecuada de los puntos fundamentales y la evolución de su derecho, y permitiéndole por otro lado, un planteamiento más exacto de los posibles problemas que se presenten, para lograr una mejor solución a las cuestiones jurídicas que se deban resolver.[118]

Es así como trataré de justificar la necesidad de robustecer el Código Penal Federal, planteando lo que otras legislaciones han trabajado para controlar estas actividades delictivas que cada vez se incrementa su comisión y en consecuencia su impunidad.

CÓDIGO PENAL ITALIANO

La legislación penal italiana especifica los delitos informáticos de manera dispersa, sin que exista un apartado especial para los delitos en cuestión, así por ejemplo el artículo 420 relacionado con atentar contra las instalaciones de servicios públicos; en su segundo párrafo refiere al daño o destrucción de sistemas informáticos o telemáticos de instalaciones de servicios públicos, es decir, datos, información o programas en ellos contenidos u otros que son relevantes. A su vez, el artículo 491 bis; se relaciona con los documentos informáticos, y sanciona a cualquier persona que los falsifica.

El numeral 615 ter, concierne al acceso no autorizado para un sistema informático o telemático; el cual sanciona a cualquier persona que tenga acceso no autorizado y se introduzca en un sistema informático o telemático protegido por medidas de seguridad; muy parecido con la legislación mexicana. Los artículos 615 quater y 615 quinquies consideran un tipo de delito relacionado con la difusión sin

[118] Marta Morineau, citando a David, Rene y Jauffret-Spinosi, Camille, en *Derecho comparado, Estudios jurídicos en homenaje a Marta Morineau*, Tomo I Derecho romano historia del derecho. Serie doctrina jurídica, Num 282. Instituto de Investigaciones Jurídicas. 2006. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/4/1855/5.pdf. Consulta 13 de Agosto 2017 21:44 hrs.

autorización de los códigos de acceso a sistemas de información o telemáticos; y sanciona a quien se beneficie a sí misma u a otros con la práctica de difundir, comunicar o entregar códigos, palabras clave u otros medios idóneos que permitan el acceso a un sistema informático o telemático, como candados de seguridad. Para proteger las telecomunicaciones, la normatividad italiana en su artículo 617 quater castiga a quien intercepte fraudulentamente comunicaciones referentes a un sistema informático o telemático o interconecte a otros sistemas, es así que impedir o interrumpir es sancionado; también el numeral 617 sexies hace lo mismo para quien falsifique, altere o suprima contenido de comunicaciones informáticas o telemáticas.

Por otro lado, el numeral 635 bis vuelve a tratar el daño de sistemas informáticos o telemáticos, sancionando a quien destruya, deteriore o marque, todo o en parte, inutilice sistemas informáticos, además de programas, información u otros datos. En este tenor el numeral 640 ter, sanciona a quien altere de cualquier modo el funcionamiento de un sistema informático o telemático o intervenga sin autorización y en cualquier modalidad los datos, información o programas.

CODIGO PENAL ESPAÑOL

La marco jurídico penal español es muy similar al mexicano con respecto de los delitos informáticos, por ejemplo, el artículo 197 relacionado con el descubrimiento y revelación de secretos, sanciona a quien sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

Así mismo, el artículo 197 bis, condena a quien vulnere las medidas de seguridad y sin estar debidamente autorizado, acceda o facilite a otro el acceso de un sistema de información, además quien intercepte transmisiones no públicas de datos informáticos. Y su correlativo 197 ter, sanciona al que sin estar debidamente autorizado, produzca, adquiera para su uso, un programa informático, una

contraseña de ordenador, un código de acceso o datos similares que permitan acceder a un sistema de información. Es importante mencionar que el numeral 573, que se relaciona con los delitos de terrorismo, especifica que se considerarán delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter.

CODIGO PENAL ALEMÁN

La normatividad alemana código penal (*Strafgesetzbuch)* regula en su artículo 202a el espionaje informático sancionando a quien sin autorización se procure para sí o para otro datos que se almacenan o trasmiten en forma electrónica o magnética y que además no estén destinados para su uso. Asimismo, a quien con el propósito, de procurarse para sí o para un tercero una ventaja económica, engañando con programas informáticos erróneos o incorrectos será acusado por estafa informática, y será sancionado de conformidad con el código 263a.

El sabotaje informático está regulado por el numeral 303b, para quien perturbe un procesamiento de datos que sea de importancia esencial para una empresa ajena, una industria ajena o una autoridad con la intención de destruir, dañar, inutilizar, eliminar o modificar un equipo de procesamiento de datos o un medio de datos, muy parecida a la legislación mexicana.

CODIGO PENAL ARGENTINO

El código penal de la nación argentina, contiene más artículos que sancionan el acceso indebido a los sistemas informáticos, así como el fraude, v.gr. el artículo 153 reprime el acceso indebido de las comunicaciones electrónicas, sea o no de carácter privado o restringido. Más preciso en el numeral 153 BIS, el cual protege a los sistemas o datos informáticos al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, ya sea de acceso restringido o de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Con respecto de la alteración, destrucción o inutilización de datos, documentos, programas o sistemas informáticos, el artículo 183 establece el castigo a quien incurra en estas conductas o bien los venda, distribuya cualquier programa con el objeto de causar daños; en este tenor, el artículo 184 sancionará si los daños se ejecutan en archivos, registros, bibliotecas, datos, documentos, programas o sistemas informáticos públicos o destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Finalmente el numeral 310 reprime las actividades de intermediación financiera sin contar con autorización emitida por la autoridad de supervisión competente utilizado internet.

CÓDIGO PENAL COLOMBIANO

El Código Penal Colombiano (Ley 599 de 2000), es sin menor duda uno de los cuerpos legislativos más desarrollado en materia de delitos informáticos, ya que contiene dos capítulos especializados con la materia, así por ejemplo en su capítulo I, de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, contempla en sus artículos 269A al 269G los siguientes tipos penales: Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales y suplantación de sitios web para capturar datos personales. Además en su capítulo II, de los atentados informáticos y otras infracciones, agrega dos tipos más en sus artículos 269I y 269J, a saber: El hurto por medios informáticos y semejantes y la Transferencia no consentida de activos.

5.6. Propuesta para el Código Penal Federal

Como se puede apreciar en las diferentes legislaciones tratadas en el punto 5.5, y haciendo un análisis comparativo, la mayoría coincide con la tipificación de conductas muy recurrentes como el robo, modificación y destrucción de información en sistemas informáticos, el fraude financiero a través de sistemas informáticos, el espionaje, el spam, las intervenciones de comunicaciones electrónicas, el terrorismo informático etcétera.

Mientras que el código penal federal mexicano, como ya se analizó en el capítulo cuarto de esta tesis, sólo regula el acceso ilícito, la modificación, destrucción, copiado de información y datos contenidos en los sistemas informáticos, consecuentemente, valdría la pena considerar la inclusión de delitos informáticos que contempla la misma Convención de Budapest, toda vez que por ser miembro el Estado mexicano de alguna manera ésta exigencia lo vincula para actualizar su normatividad local para estar acorde a las nuevas exigencias globales en materia de ciberdelincuencia, así por ejemplo, me atrevería a sugerir la reforma del Título Noveno que ahora se intitula "*Revelación de secretos y acceso ilícito a sistemas y equipos de informática"* y cambiarlo a "*Revelación de secretos y Delitos informáticos"* , así mismo el Capitulo II "*Acceso ilícito a sistemas y equipos de informática"* por "Delitos informáticos"; de tal suerte que en este capítulo II contemplará, además de los que ya tiene, los siguientes Tipos Penales:

211 BIS 8. FALSIFICACIÓN INFORMÁTICA

Sancionando al que cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que se tomen en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles.

211 BIS 9. FRAUDE INFORMÁTICO

Sancionar al que mediante la introducción, alteración, borrado o supresión de datos informáticos; o con cualquier tipo de interferencia en el funcionamiento de un sistema informático, y con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

211 BIS 10. PORNOGRAFÍA INFANTIL INFORMÁTICA

Sancionar al que produzca, oferte, ponga a disposición, difunda, transmita, adquiera o posea pornografía infantil a través de un medio o sistema informático para uno mismo o para otra persona.

Se entenderá como pornografía infantil a todo material pornográfico que contenga la representación visual de: i) un menor comportándose de una forma sexualmente explícita; ii) una persona que parezca un menor comportándose de una forma sexualmente explícita.

211 BIS 11. PROPIEDAD INTELECTUAL INFORMÁTICA

Sancionar las conductas que se cometan deliberadamente, a escala comercial y por medio de un sistema informático de la reproducción sin autorización de las creaciones de la mente, invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio.

211 BIS 12. ENVÍO DE COMUNICACIONES PUBLICITARIAS O PROMOCIONALES POR CORREO ELECTRÓNICO

Sancionar el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. En otras palabras, se desautorizan las comunicaciones dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

211 BIS 13. USO DE PROGRAMAS INFORMÁTICOS MALICIOSOS.

Para imponer una sanción privativa de la libertad a quien produzca, trafique, adquiera, distribuya, venda, envíe, introduzca al territorio nacional software malicioso u otros programas de computación cuyos efectos sean dañinos en los sistemas o equipos de cómputo propiedad ajena.

De manera concreta, en este último capítulo nos hemos dado cuenta que la tecnología cambia constantemente, lo que significa que los ciberataques también evolucionan; continuamente se descubren nuevas vulnerabilidades y métodos de ataque. La seguridad se ha convertido en una preocupación importante para las personas y las empresas, para esta últimas es prioritario debido a la reputación y el impacto financiero que sufren. Sabemos que los ataques están dirigidos a redes débiles y datos confidenciales vulnerables.

Si bien es cierto que en este capítulo se desarrolló la propuesta toral de la persecución de los delitos que se cometen a través de los medios informáticos proporcionando los elementos para la investigación, análisis, registro e interpretación de evidencia digital, así como las herramientas para su materialización; no menos cierto es que resulta insuficiente con la persecución sino que hace falta el marco legal a través del derecho penal para contrarrestar las conductas ilícitas y castigar su consumación.

CONCLUSIONES

La evidente necesidad de ampliar el catálogo de tipos penales, relacionados con la informática, en el Código Penal Federal se vuelve una prioridad para el legislador debido a que hoy por hoy la mitad de la población tiene una relación directa con el ciberespacio, es decir que en México se estima que: hay alrededor de 65 millones de usuarios de servicios informáticos, el 65 % de los correos electrónicos son spam, uno de cada 506 correos contiene malware, los costos financieros de la ciberdelincuencia ascendieron a 5 mil 500 millones de dólares; en un minuto hay 20 víctimas de defraudación en internet, 83 mil ventas electrónicas, 20 millones de fotos transferidas, 330 mil twits, mil 300 nuevos usuarios móviles[119]. A medida que un creciente número de delitos involucran evidencia electrónica, la necesidad de regular cualquier actividad en la web, se convertirá en una exigencia y no sólo para el delito informático, sino también para todas las conductas ilícitas en general.

Por lo anterior, considero que el legislador tiene una tarea por demás complicada, dada la época que estamos viviendo, sobre todo en México, con el advenimiento y fortalecimiento de los Derechos Humanos; no es nada sencillo establecer restricciones a esos derechos que los instrumentos internacionales (como el Pacto de San José) han ratificado a través de la jurisprudencia de la CoIDH. Así surge la necesidad de realizar un balance entre la libertad y la seguridad, "*Una de las principales cuestiones a las que se enfrenta la sociedad contemporánea en las esferas de la teoría y la práctica política, el derecho, la filosofía y los derechos humanos es si existe un equilibrio aceptable entre las necesidades de seguridad nacional y la protección de las libertades civiles"*[120]*.* Si bien es cierto que México requiere actualizar su normatividad penal en el contexto tecnológico, no menos

[119] http://hemeroteca.oem.com.mx/laprensa/20170814/index.html. Fecha de consulta 14 de Agosto 2017, 21:00 hrs.

[120] Moss, Kate, Balancing Liberty and Security, Human Rights, Human Wrongs, Crime Prevention and Security Management Martin Gill series Editor, Hampshire, England, 2011, p. 1 "*One of the major questions facing contemporary society in the areas of political theory and practice, law, philosophy and human rights is whether there is an acceptable balance between national security needs and the protection of civil liberties*"

cierto es que esto debe ocurrir a la luz de los derechos fundamentales que se han consagrado en sede constitucional con un carácter de progresividad.

Esta tesis sólo mostró de manera general qué son los delitos informáticos, cuál es su mecanismo de consumación y medio de comisión; qué organizaciones internacionales regulan esta conducta, los elementos estructurales de la Convención contra la ciberdelincuencia, cuáles son los delitos informáticos de mayor recurrencia; también, se atendió la situación de México en materia normativa, se desarrolló una propuesta de estudio técnico de los tipos penales en materia de ciberdelincuencia dentro del Código Penal Federal, se enlistó una serie de propuestas de tipos penales necesarios para dar cumplimiento a estándares internacionales y sobre todo a conductas que cada vez serán tema cotidiano; asimismo, se desarrollaron aspectos técnicos en materia de tecnología de las telecomunicaciones, necesarios para quienes buscan adentrarse al tema del ius puniendi en materia de redes de información. Por lo que a manera de recapitulación llego a las siguientes conclusiones:

PRIMERA. Es claro que en esta época globalizada ninguna persona debe quedarse al margen de las tecnologías de la información, así como el Derecho; éstas han regulado y cambiado la conducta humana que cada vez es más grande su dependencia, en cualquier ámbito de la vida, financiera, educativa, laboral, comunicación, entretenimiento, de manera tal que, podríamos deducir sin temor a errar que para que una persona pueda ser considerada competente en cualquier actividad profesional, el conocimiento de tecnologías de la información necesariamente debe ser parte de su perfil curricular.

No hay manera de evitar esta tendencia pues el ser humano provoca la interconectividad de las cosas, automatizando, instalando ojos electrónicos o cámaras que le ayudan a tener control vehicular en las calles, sirviéndose de androides para facilitar el trabajo rudo, y sobre todo para acortar la distancia intercultural en un planeta cada vez más achicado por el campo de las telecomunicaciones.

SEGUNDA. Dada la tendencia inevitable en el desarrollo de las telecomunicaciones y la interconectividad de dispositivos informáticos, las organizaciones delincuenciales proliferarán aún más, y la vulnerabilidad de los bienes jurídicamente tutelados también crecerá debido a la sofisticada y compleja actividad que se desarrolla en las nubes de comunicación que implica la internet. Es por ello que urge tomar medidas acertadas para contrarrestar esta tendencia, como las desarrolladas en este trabajo de tesis. Donde por un lado, el conocimiento preciso y accesible de los riesgos de ataques informáticos que vulneran la información confidencial de las personas físicas, morales y oficiales, nos lleve a decisiones adecuadas en torno a la seguridad y la utilización de mecanismos técnicos de protección informática; por el otro, a establecer nuevos tipos penales que faciliten la labor de la procuración e impartición de justicia de la nación mexicana.

TERCERA. El trabajo del legislador mexicano debe estar enfocado a crear tipos penales especiales cuyo medio comisivo es el internet y las redes informáticas, como la pornografía infantil, el fraude financiero, los correos basura, robo de identidad, sabotaje, piratería, acoso sexual, incluso terrorismo. Asimismo, crear un capítulo especializado en el Código Penal Federal, que contengan estas normas prohibitivas específicas, de tal suerte que exista certeza jurídica para los millones de usuarios que día a día navegan a través de la realidad virtual. Porque sólo a través de un marco normativo robusto que regule cualquier conducta que lesione los intereses de las víctimas y que tutele esas categorías axiológicas que la sociedad de la información ha definido, es así como una nación como México podría dar un paso enorme para acortar la brecha del rezago tecnológico que tenemos con respecto de otros países desarrollados y porque además el Estado mexicano ya forma parte de un tratado internacional en la materia que lo obliga. No obstante a que han pasado ocho años desde que Téllez Valdéz escribió el siguiente argumento, hoy más que nunca cobra mayor vigencia para reconsiderarlo.

> *Los autores de esos delitos deben ser identificados y llevados a juicio y los tribunales han de disponer de sanciones adecuadas y proporcionadas. Se enviará así un claro mensaje disuasivo a los autores potenciales de ataques contra los sistemas de información; además los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información.*[121]

CUARTA. Si bien es cierto que cada vez estas conductas delictivas se vuelven más sofisticadas y que evitan ser rastreadas con mecanismos de encriptamiento y anonimato, también lo es que, el mundo de los sistemas de seguridad informática va avanzando con pasos firmes, al crear herramientas como wireshark para su búsqueda en el ciberespacio; en este aspecto la tesis proporcionó un panorama general sobre las ventajas de la aplicación para perseguir conductas que emplean los ataques activos, rastrear mediante los indicios digitales que dejan los ciberdelincuentes al cometer el injusto penal, hasta determinar el origen y ubicación del ataque, evidentemente esta comprensión no es factible si no se cuenta con los conocimientos básicos sobre la comunicación de las computadoras a través de sus protocolos. El tema de la prevención cobra una relevancia de gran magnitud, protegiendo nuestros sistemas informáticos ya sea en casa, en el trabajo o en el negocio; crear hábitos de protección salvaguardando información confidencial, discriminando la información que se comparte en las redes sociales, supervisar la conexión de las niñas y los niños en la web, porque la oportunidad que tenemos en nuestros días de achicar las distancias en el mundo, es gracias a las redes de telecomunicaciones lo que debe representar un privilegio no una preocupación.

El futuro nos alcanzó y la tendencia es irreversible, la era donde todo está interconectado es una realidad, donde las casas inteligentes, los Smartphone, el ciberespacio, la inteligencia artificial y el internet de las cosas, son los temas y es el lenguaje de hoy; donde todos estamos llamados a participar para bien o para mal, sin alternativa y donde además no hay escapatoria.

[121] Téllez Valdés, op. cit. nota 60, p.206

GLOSARIO

ALGORITMO. Es un conjunto secuencial de instrucciones o indicaciones bien definidas, ordenadas de manera lógica que permite llevar a cabo una actividad mediante pasos sucesivos que no generen dudas a quien deba hacer dicha actividad.

ANDROID. Es un sistema operativo basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, tabletas y también para relojes inteligentes, televisores y automóviles.

ASIC. Un Circuito Integrado para Aplicaciones Específicas (o ASIC, por sus siglas en inglés) es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general. Se usan para una función específica. Por ejemplo, un chip diseñado únicamente para ser usado en un teléfono móvil es un ASIC.

BASE DE DATOS. Conjunto ordenado y clasificado de datos, en informática las bases de datos están en sistemas binarios, solución al problema del almacenamiento de datos.

BACKBONE. La palabra backbone (columna vertebral) se refiere a las principales conexiones troncales de Internet.

BIT. Acrónimo de *Binary digit* o dígito binario, Un bit es un dígito del sistema de numeración binario.

BOTNET. Es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.

BRIDGE. En telemática, bridge o puente de red es un dispositivo para interconexión de redes locales.

CD-RW. Estos discos compactos también presentan una capacidad de 650 MB pero tienen la ventaja de ser regrabados, por lo que su contenido puede modificarse tantas veces como su usuario lo precise.

COMANDO. Es una instrucción contenida en un programa informático para que la computadora realice una tarea.

CPU. La unidad central de procesamiento o unidad de procesamiento central (conocida por las siglas CPU, del inglés: central processing unit), es el hardware dentro de un ordenador u otros dispositivos programables, que interpreta las instrucciones de un programa informático.

CLÚSTER. Referido a un sistema de archivos, es un conjunto contiguo de sectores que componen la unidad más pequeña de almacenamiento de un disco.

DDoS, Ataque. En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (por sus siglas en inglés), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los

usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado. Un ejemplo notable de ello se produjo el 27 de marzo de 2013, cuando el ataque de una empresa a otra inundó la red de correos basura provocando una ralentización general de Internet e incluso llegó a afectar a puntos clave como el nodo central de Londres.

DIRECCIÓN MAC. Es un identificador único, de 6 bloques de dos caracteres hexadecimales asignada a una tarjeta o dispositivo de red. (v.g. D4:63:FE:B7:9C:FA).

DISQUETE. Este dispositivo de almacenamiento está conformado por un disco de material magnético en el que se graba y lee la información.

DRM. Del inglés *digital rights management*, también llamado programas anticopia, es un término que se refiere a las tecnologías de control de acceso usadas por editoriales y titulares de derechos de autor para limitar el uso de medios o dispositivos digitales a personas o equipo no autorizados.

eBAY. Es un sitio destinado a la subasta de productos a través de Internet. Es uno de los pioneros en este tipo de transacciones, fundado en el año 1995.

ENCRIPTAR. Llamado cifrado, es un procedimiento que utiliza una clave para transformar un mensaje, para que resulte incomprensible durante su transmisión.

ext4 (del inglés *fourth extended filesystem* o «cuarto sistema de archivos extendido») es un sistema de archivos transaccional (en inglés journaling), anunciado el 10 de octubre de 2006 por Andrew Morton, como una mejora compatible de ext3.

FAT32. (del inglés *file allocation table*), es un sistema de archivos desarrollado para MS-DOS, así como el sistema de archivos principal de las ediciones no empresariales de Microsoft Windows hasta Windows Me.

FIREWALL. Un corta-fuegos es un elemento de una red que evita o bloquea el acceso no autorizado de paquetes de información, permitiendo al mismo tiempo comunicaciones seguras.

FREEBSD. FreeBSD es un sistema operativo libre para computadoras basado en las CPU de arquitectura Intel, incluyendo procesadores Intel 80386, Intel 80486 (versiones SX y DX), y Pentium.

GPRS. El servicio general de paquetes vía radio, en inglés: General Packet Radio Service (GPRS), fue creado en la década de los años 1980. Es una extensión del "Sistema Global para comunicaciones Móviles" (Global System for Mobile Communications o GSM) para la transmisión de datos mediante conmutación de paquetes.

HACKER. Experto en crear software que manipula o modifican los usos de las computadoras de modo que éstas puedan emplearse para fines lícitos o ilícitos.

HFS. Sistema de Archivos Jerárquico o *Hierarchical File System*, es un sistema de archivos desarrollado por Apple Inc. para su uso en computadores que corren Mac OS.

HOST. El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

HTTP. Es el protocolo de comunicación que permite las transferencias de información en la World Wide Web.

ISP. El proveedor de servicios de Internet (Internet Service Provider) brinda conexión a Internet a sus clientes, a través de diferentes tecnologías como DSL, 4G LTE, dial-up, etcétera.

1Mbps. Un millón de bits por segundo.

LAN. Red de área local o LAN (por las siglas en inglés de Local Area Network) es una red de computadoras que abarca un área reducida a una casa, un departamento o un edificio.

LINUX. Linux es un núcleo de libre distribución y mayormente libre semejante al núcleo de Unix.

LOGS. En informática, se usa el término log, historial de log o registro a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos (eventos o acciones) que afectan a un proceso particular.

Mac OS X. MacOS, anteriormente denominado OS X e inicialmente Mac OS X, es un entorno operativo basado en Unix, desarrollado, comercializado y vendido por Apple Inc.

MEMORIA RAM. Esta memoria es de lectura y de escritura, por lo que se la llama de acceso aleatorio.

MEMORIA ROM. Esta es la memoria utilizada para almacenar el programa de básico de iniciación y tiene la tarea de identificar a los distintos dispositivos.

MICROSOFT. Es una empresa multinacional de origen estadounidense, fundada el 4 de abril de 1975 por Bill Gates y Paul Allen.

NetBSD. Es un sistema operativo de la familia Unix de código abierto y libre, y, a diciembre de 2008, disponible para más de 56 plataformas de hardware.

NTFS. (siglas en inglés de *New Technology File System*) es un sistema de archivos de Windows NT incluido en las versiones de Windows NT 3.1, Windows NT 3.5, Windows NT 3.51, Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008, Windows Vista, Windows 7, Windows 8 y Windows 10.

PROTOCOLO DE COMUNICACIONES. En informática y telecomunicación, al conjunto de reglas y estándares que controlan la secuencia de mensajes que ocurren durante una comunicación entre entidades que forman una red, como teléfonos o computadoras.

SEGURIDAD INFORMÁTICA. Conocida como ciberseguridad o seguridad de tecnologías de la información, se enfoca en la protección de la infraestructura de la red computacional, en especial de la información.

SISTEMA BINARIO: es un sistema de numeración en el que los números se representan utilizando solamente, dos cifras: cero y uno (0 y 1). Es utilizado en las computadoras, debido a que estas trabajan internamente con dos niveles de voltaje (5v = 1 y 0v= 0).

SMS. Es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos, conocidos como mensajes de texto.

SNIFFER. Es un programa informático que registra la información que envían los periféricos, así como la actividad realizada en un determinado ordenador.

SNORT. Es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión).

SOLARIS. Es un sistema operativo de tipo Unix desarrollado desde 1992 inicialmente por Sun Microsystems y actualmente propiedad de Oracle Corporation.

SPAM. El spamming es el envío de grandes cantidades de información basura, habitualmente de tipo publicitario, o correo basura, que perjudican de alguna manera a la computadora receptora.

SWITCH. Conmutador es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

OpenBSD. Es un sistema operativo libre tipo Unix multiplataforma, basado en 4.4BSD. Es un descendiente de NetBSD, con un foco especial en la seguridad y la criptografía.

TDMA. El acceso múltiple por división de tiempo (Time Division Multiple Access) es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión.

TCP. Protocolo de Control de Transmisión (Por sus siglas en inglés, Transmission Control Protocol) es uno de los protocolos fundamentales en Internet.

TIC. El término tecnologías de la información y la comunicación (Por sus siglas en inglés TIC o TICs) El conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información, se ha matizado de la mano de las TIC, pues en la actualidad no basta con hablar de una computadora cuando se hace referencia al procesamiento de la información.

UNIX. Es un sistema operativo portable, multitarea y multiusuario.

UNODC. Del inglés, *United Nations Office on Drugs and Crime*. Oficina de Drogas y Crimen de las Naciones Unidas.

URL. Cadena de caracteres que se asignada de manera única a cada uno de los recursos de información disponibles en Internet. (v.g. http://www.posgrado.derecho.unam.mx/)

UDP. User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su encabezado.

ROUTER. Un router, también conocido como enrutador, encaminador o rúter, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI.

VIRUS INFORMÁTICO. Software o programas que al ejecutarse alteran el funcionamiento normal de una computadora, y pueden destruir, de manera intencionada, los datos almacenados en ella.

FUENTES DE CONSULTA

BIBLIOGRÁFICAS

1. Aguilar López, Miguel Ángel. *El delito y la responsabilidad penal, teoría, jurisprudencia y práctica*, Séptima edición, Editorial Porrúa, México, 2015.

2. Akhgar, Babak, et al, *Ciber Crime and Ciber Terrorism Investigator's HandBook*, Copyright Elsevier Inc. USA, 2014.

3. Amoroso, Edward G., *Cyber Attacks, Protecting national infrastructure*, Elseiver, USA, 2011.

4. Bryant, Robin, P., *Investigating Digital Crime*, Canterbury Christ Church University, UK. John Wiley & sons Ltd. 2008.

5. Borja Merino Febrero, *Análisis De Tráfico con Wireshark*, Instituto Nacional de Tecnología de la Comunicación, Febrero, 2011.

6. Carvallo Yáñez, Erick, *Nuevo derecho bancario y bursátil mexicano, Teoría y práctica de las agrupaciones financieras, las instituciones de crédito y las casa de bolsa*, Editorial Porrúa, novena edición, México, 2014.

7. Casey, Eoghan, *Digital evidence and computer crime, Forensic science, computers and the internet*, Third Edition, Elsevier, USA, 2011.

8. Cienfuegos Salgado, David y Vázquez Mellado, Julio Cesar, *Vocabulario Judicial*, Instituto de la Judicatura Federal – Escuela Judicial. Primera edición, México, 2014.

9. Cury Ursúa, Enrique, *Derecho Penal Parte General*, 2ª Edición, Editorial Jurídica de Chile, Tomo I, Santiago, Chile, 1992.

10. Chiesa, Raoul, et al, *Profiling Hackers, The Science of Criminal Profiling as Applied to the World of Hacking*, Taylor & Francis Group, LLC, 2009.

11. David S. Wall. *Cybercrime, the transformation of Crime in the information Age*. Polity Press. Cambridge UK. 2007.

12. De Pina Vara, Rafael, *Diccionario de Derecho*, 37ª Edición, segunda reimpresión, Editorial Porrúa, México 2012.

13. Díaz Aranda, Enrique y Roxin, Claus, *Teoría de la caso y del delito en el proceso penal acusatorio*, Straf, Primera edición, México 2015.

14. Díaz Aranda, Enrique, *Cuerpo del delito, probable responsabilidad y la reforma constitucional de 2008*, Instituto de Investigaciones Jurídicas, serie Estudios Jurídicos, Número 147. México, 2009.

15. Díaz García, Alexander, *Derecho informático, elementos de la informática jurídica*, 1ª Reimpresión, Editorial Leyer, Bogotá 2012.

16. E. Douglas, John, et al, *Crime classification manual, a standar system for investigating, and classifying violent crimes*, Second Edition, John Wiley & Sons, Inc. San Francisco, CA, 2006.

17. Gercke, Marco, *Understanding cybercrime: phenomena, challenges and legal response*. The ITU Telecommunication Development Bureau Publication. September 2012.

18. Gil García, José Ramón, et al, *Tecnologías de Información y Comunicación en la Administración Pública: Conceptos, Enfoques, Aplicaciones y Resultados*, INFOTEC Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, Primera edición, México, 2017.

19. Gómez Vieites, Álvaro, *Enciclopedia de la seguridad informática*, 2a Edición Actualizada, Alfaomega, 2011

20. Greenblatt, Sara, et al, *Comprehensive study on cybercrime*. United Nations Office on Drugs and Crime, Draft, February 2013.

21. González Rodríguez, Patricia L. *La policía investigadora en el sistema acusatorio mexicano*, Instituto de Investigaciones Jurídicas, Colección monográfica de juicios orales núm 7, UNAM, México 2013.

22. Gutiérrez Gallardo, Claudio, *Cómo funciona la Web, Centro de Investigación de la Web,* Departamento de Ciencias de la Computación Universidad de Chile, 2008.

23. Haydée Di Iorio, Ana, et al, *El rastro digital del delito, aspectos técnicos, legales y estratégicos de la Informática Forense*. Grupo De Investigación en Sistemas Operativos e Informática Forense, Universidad FASTA, 2016.

24. Jacobs, Don, *Analyzing Criminalminds, Forensic Investigative Science for the 21st Century*, Brain and Evolution Patrick McNmara, Series Editor Praeger. USA 2011.

25. James Curran, Natalei Fenton and Des Freedman, *Misunderstanding the Internet*. Taylor&Francis Group, Second Edition, New York,NY. 2016.

26. Jiménez Martínez, Javier. *La Teoría Del Delito*, *Aproximación al estado de la discusión.* Editorial Porrúa. Primera edición. México 2010.

27. J. Cano M., Jeimy, *Computación Forense*, *descubriendo los rastros informáticos*, 2a Ed. Editorial Alfaomega, México, 2015.

28. K. Jaishankar, *Cyber Criminology, Exploring Internet Crimes and Criminal Behavior*, Taylor and Francis Group, LLC, Printed in the United States of America, 2011.

29. Lázaro Domínguez, Francisco, *Introducción a la Informática forense*, Editorial RA-MA, Madrid, 2012.

30. López Betancourt, Eduardo, *Delitos en particular 4*, Tercera edición, Editorial Porrúa México, 2016.

31. Malo Camacho, Gustavo, *Derecho penal mexicano*, quinta edición, editorial Porrúa, México 2003.

32. Marta Morineau, *Derecho comparado, Estudios jurídicos en homenaje a Marta Morineau*, Tomo I Derecho romano historia del derecho. Serie doctrina jurídica, Núm. 282. Instituto de Investigaciones Jurídicas. 2006.

33. Miller, Mark, *Internet Technologies Handbook, Optimizing the IP Network*, John Wiley & Sons, Inc,Hoboken, New Jersey, 2004.

34. Montoya Piña, Javier Omar, *Delitos federales cometidos a través de medios informáticos*, Editorial Flores Editor y Distribuidor, SA de CV., México, 2015.

35. Moriarty, Laura, *Controversies in Victimology*, Second Edition, Matthew Bender & Company, Inc.,2008.

36. Moss, Kate, *Balancing Liberty and Security, Human Rights, Human Wrongs*, Crime Prevention and Security Management Martin Gill series Editor, Hampshire, England, 2011.

37. Mozayani, Ashraf and Noziglia, Carla, *The forensic laboratory handbook: procedures and practice*. Steven B. Karch, MD, Series Editor, Humana Press Inc. New Jersey. 2006.

38. Nava Garcés, Alberto Enrique, *Dogmática penal y teoría del delito, crítica y método*, 1a edición, Editorial Porrúa, México 2012.

39. Nava Garcés, Alberto E., *Delitos informáticos*, Tercera Edición, Editorial Porrúa, México, 2016.

40. Nieves, Ricardo, *Teoría del Delito y Práctica penal, reflexiones dogmáticas y mirada crítica*. Escuela Nacional del Ministerio Público, Santo Domingo, República Dominicana, Editora Centenario, S. A., 2010.

41. Ojeda Paullada, Pedro, *Concepto de Procuraduría*, Instituto Nacional de Administración Pública, Núm. 97 revista de administración pública, México, 1998.

42. Orellana Wiarco, Octavio A., *Curso de derecho penal, Perte general*, Editorial Porrúa, Quinta edición corregida y aumentada. México, 2011.

43. Palomá Parra, Luis Orlando, *Delitos informáticos en el ciberespacio*, Ediciones Jurídicas Andrés Morales, Colombia, 2012.

44. Pichardo Pagaza, Ignacio, *Introducción a la nueva administración pública de México*, Volumen 1, Instituto Nacional de Administración Pública, segunda edición, corregida y aumentada, México, abril 2002.

45. Roxin, Claus. *Derecho Penal parte general, tomo 1 fundamentos, La estructura de la teoría del delito*. Traducción de la 2a edición alemana, Editorial Civitas, Madrid España, 1997.

46. Téllez Carbajal, Evelyn, *Derecho y TIC. Vertientes actuales*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, núm. 751, México 2016.

47. Téllez Valdés, Julio, *Derecho informático*, cuarta edición, Editorial Mc Graw Hill, México, 2009.

48. Sergio García Ramírez, Sergio y Islas de González Mariscal, Olga. *Derecho Penal Y Criminalística*, XII Jornadas sobre Justicia Penal. Instituto de Investigaciones Jurídicas, Serie de Estudios Jurídicos, Núm. 2018, UNAM, México 2012.

49. Simoneau, Paul. The OSI Model: *Understanding the Seven Layers of Computer Networks*. Global Knowledge, 2006.

50. Welzel, Hans, *Derecho Penal parte general*, traducción de Carlos Fontán Balestra, Editorial Roque Depalma, Buenos Aires, Argentina 1956.

51. Watson, David and Jones, Antrew, *Digital Forensics Processing and Procedures, Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*, Elseiver, Inc. USA 2013.

52. W. Osterburg, James and H. Ward, Richard, *Criminal investigation a method for reconstructing the past,* Sixth Edition, AP Anderson publishing, NJ 2010.

LEGISLACIÓN NACIONAL

53. Código Nacional de Procedimientos Penales. (Publicado en el Diario Oficial de la Federación el 5 de marzo de 2014. Última reforma publicada DOF 17-06-2016)

54. Código Penal Federal. (Publicado en el Diario Oficial de la Federación el 14 de agosto de 1931; Última reforma publicada DOF 26-06-2017)

55. Constitución Política de los Estado Unidos Mexicanos. (Publicada en el Diario Oficial de la Federación el 5 de febrero de 1917; Última reforma publicada DOF 24-02-2017)

56. Ley de Firma Electrónica Avanzada. (Publicada en el Diario Oficial de la Federación el 11 de enero de 2012)

57. Ley de Instituciones de Crédito. (Publicada en el Diario Oficial de la Federación el 18 de julio de 1990; Última reforma publicada DOF 17-06-2016)

58. Ley de Instituciones de Seguros y de Fianzas. (Publicada en el Diario Oficial de la Federación el 4 de abril de 2013; Ultima reforma publicada DOF 10-01-2014)

59. Ley de la Comisión Nacional Bancaria y de Valores. (Publicada en el Diario Oficial de la Federación el 28 de abril de 1995; Última reforma publicada DOF 10-01-2014)

60. Ley de los Sistemas de Ahorro para el Retiro. (Publicada en el Diario Oficial de la Federación el 4 de abril de 2013; Ultima reforma publicada DOF 10-01-2014)

61. Ley de Protección al Ahorro Bancario. (Publicada en el Diario Oficial de la Federación el 19 de enero de 1999; Última reforma publicada DOF 10-01-2014)

62. Ley de Protección y Defensa al Usuario de Servicios Financieros. (Publicada en el Diario Oficial de la Federación el 18 de enero de 1999; Última reforma publicada DOF 10-01-2014)

63. Ley de Seguridad Nacional. (Publicada en el Diario Oficial de la Federación el 31 de enero de 2005; Última reforma publicada DOF 26-12-2005)

64. Ley Federal Contra la Delincuencia Organizada. (Publicada en el Diario Oficial de la Federación el 7 de noviembre de 1996; Última reforma publicada DOF 07-04-2017)

65. Ley Federal de Derechos. (Publicada en el Diario Oficial de la Federación el 31 de diciembre de 1981; Última reforma publicada DOF 07-12-2016)

66. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (Publicada en el Diario Oficial de la Federación el 5 de julio de 2010)

67. Ley Federal de Responsabilidad Patrimonial del Estado. (Publicada en el Diario Oficial de la Federación el 31 de diciembre de 2004; Última reforma publicada DOF 12-06-2009)

68. Ley Federal de Telecomunicaciones y Radiodifusión. (Publicada en el Diario Oficial de la Federación el 14 de julio de 2014; Última reforma publicada DOF 27-01-2017)

69. Ley Federal de Transparencia y Acceso a la Información Pública. (Publicada en el Diario Oficial de la Federación el 9 de mayo de 2016; Última reforma publicada DOF 27-01-2017)

70. Ley Federal del Derecho de Autor. (Publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996; Última reforma publicada DOF 13-01-2016)

71. Ley General de Víctimas. (Publicada en el Diario Oficial de la Federación el 9 de enero de 2013; Última reforma publicada DOF 03-01-2017)

72. Ley General del Sistema Nacional de Seguridad Pública. (Publicada en el Diario Oficial de la Federación el 2 de enero de 2009; Última reforma publicada DOF 26-06-2017)

73. Ley General para Prevenir, Sancionar y Erradicar los delitos en Materia de Trata de Personas. (Publicada en el Diario Oficial de la Federación el 14 de junio de 2012; Última reforma publicada DOF 19-03-2014)

74. Ley Orgánica de la Procuraduría General de la República. (Publicada en el Diario Oficial de la Federación el 29 de mayo de 2009; Última reforma publicada DOF 18-07-2016)

LEGISLACIÓN EXTRANJERA

75. Código Penal Alemán (Strafgesetzbuch, Änderungen seit dem 1.10.2000)

76. Código Penal Colombiano (Vigente, Publicada en el diario oficial número 44.097 del 24 de julio de 2000)

77. Código Penal de la Nación Argentina (LEY 11.179 T.O. 1984 actualizado)

78. Código Penal español. (Código reformado y en vigor el 23-12-2010)

79. Código Penal Italiano (Codice Penale Ultimo assiornamento 3 marzo 2016)

ELECTRÓNICA

80. www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx

81. www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

82. www.unodc.org/unodc/es/

83. http://www.milenio.com/policia/Cibercriminalidad-Mexico-adhiere-Convenio_de_Budapest-PGR-delitos_informaticos-delitos_en_internet_0_274173006.html

84. http://ru6.cti.gr/bouras-old/WP_Simoneau_OSIModel.pdf.

85. https://docstore.mik.ua/orelly/networking/puis/ch16_02.htm

86. https://archivos.juridicas.unam.mx/www/bjv/libros/7/3169/15.pdf

87. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

88. http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad

89. http://www5.diputados.gob.mx/index.php/esl/Comunicacion/Boletines/2016/Noviembre/29/2661-Delito-de-usurpacion-de- identidad-sera-castigado-con-uno-a-seis-anos-de-prision

90. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

91. http://www.toptenreviews.com/

92. https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf

93. https://uvadoc.uva.es/bitstream/10324/13740/1/TFG-D_0124.pdf

94. https://previa.uclm.es/profesorado/licesio/Docencia/IB/IBTema1.pdf

95. http://www.oas.org/juridico/english/cyb_pry_convenio.pdf

96. http://historico.juridicas.unam.mx/publica/librev/rev/rap/cont/97/pr/pr2.pdf

97. https://www.gob.mx/sesnsp/estructuras/dr-ricardo-corral-luna

98. https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

99. https://archivos.juridicas.unam.mx/www/bjv/libros/4/1855/5.pdf

100. http://hemeroteca.oem.com.mx/laprensa/20170814/index.html

101. https://www.cisco.com/c/es_mx/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

102. https://www.iana.org/

103. http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-ports.html

104. https://www.iso.org/ics/35.100/x/

105. https://www.iacis.com

INSTRUMENTOS INTERNACIONALES

106. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.I.2003.

107. Convenio Sobre La Ciberdelincuencia, Budapest, 23.XI.2001

108. Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.

109. ICT Applications and Cybersecurity Division Policies and Strategies Department ITU Telecommunication Development Sector, Draft April 2009.

110. International TelecommunicationUnion Cybercrime Legislation Resources, understanding cybercrime: A GUIDE FOR DEVELOPING COUNTRIES, ICT Applications and Cybersecurity Division Policies and Strategies Department.

111. ITU Telecommunication Development Sector, Draft April 2009

112. Naciones Unidas A/CONF.213/9, 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador (Brasil), 12 a 19 de abril de 2010.

113. U.S. Department of Justice, Federal Bureau of Investigation, Internet Crime Report 2015.

114. Unión Internacional de Telecomunicaciones, Lista De Recomendaciones UIT-T Edición 2004-1.

115. United Nations Office On Drugs And Crime, Vienna. UNODC Annual Report Covering activities during 2015.