UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

*"**Análisis jurídico sobre la regulación penal a nivel local y federal sobre los delitos informáticos y el uso delincuencial del internet".***

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

P R E S E N T A

ERICK GUSTAVO GONZÁLEZ ROJAS

ASESOR:

LICENCIADO RODRIGO RINCÓN MARTÍNEZ.

Mayo 2017.

SANTA CRUZ ACATLÁN, NAUCALPAN, ESTADO DE MÉXICO.

AGRADECIMIENTOS.

A mi madre, quien desde que comencé mi andar por la educación me ha enseñado el valor del estudio y el esfuerzo, así como el de la responsabilidad. Gracias por todo el amor que me das porque sin ti no podría terminar esta etapa en mi vida. Todo te lo debo a ti, y como siempre me lo decías, “Mamá siempre tiene la razón”.

A mi padre, quien gracias a él soy el hombre que hoy está aquí, y gracias a él, seré el hombre que marque el rumbo de mi vida. Gracias por el amor, por la enseñanza del coraje, por el aprendizaje y por todos los momentos que desde pequeño compartí contigo, hoy este éxito es tuyo, pues tú eres mi mejor amigo y así será siempre.

A mi hermano, quien representa ese constante recordatorio de ser un ejemplo a seguir, pues tú eres mi motor para trazar el camino correcto, solo para ti. Gracias por todo, te amo.

A mi novia Ale, por aparecer en mi vida universitaria en el último año y ser mi compañera profesional en los proyectos que juntos iniciamos, por la enseñanza constante y la motivación a seguir sin parar, por tu paciencia, comprensión, respeto y amor. Gracias por todo, amor. Te amo mucho.

Al Licenciado Rodrigo Rincón Martínez , por darme la oportunidad y la confianza de guiar este trabajo, por su disposición y su paciencia. Sinceramente Gracias.

A la profesora Gabriela Milagrosa Caballero Salia, por su apoyo constante, por su comprensión y su cariño. Por usted mucho de esto se logró. Sinceramente Gracias.

A la Universidad Nacional Autónoma de México, en particular a la Facultad de Estudios Superiores Acatlán, por darme la única y valiosa oportunidad de estudiar la licenciatura, por permitirme conocer muy buenos amigos y compañeros, por los grandes profesores que conocí, a todos ellos los recuerdo con mucho aprecio, cariño y admiración. Gracias por formarme como abogado.

INDICE

INTRODUCCIÓN.

El presente trabajo de investigación surge por la inquietud de analizar la relación entre el mundo jurídico, es decir, el mundo del Derecho y la sociedad de la información, es decir, la dinámica que la sociedad actual tiene ra prácticamente todas sus actividades diarias algún elemento tecnológico que favorece el desarrollo, propagación y distribución de la información, específicamente en el ámbito penal.

Es conocido ampliamente que existen diversas capitulaciones al respecto, donde se han abordado temas relacionados a este tópico, sin embargo, al adentrarse al mismo, se aprecia que existe una alta tasa de impunidad, sobre el uso delincuencial que se le da a la información y al material multimedia intercambiado en las interconexiones de redes de información.

Si bien es cierto, que existen disposiciones en los diversos ordenamientos jurídicos sustantivos en materia penal de las diversas entidades federativas, así como el Código Penal Federal, también lo es que dichas disposiciones en ocasiones se ven rebasadas por la realidad, pues si el Derecho es una disciplina que avanza, cambia y se adapta al cambio constante de la sociedad, también lo es que el avance tecnológico siempre en todas las veces es mucho mayor del crecimiento que como sociedad tenemos y no se diga, del avance que como Derecho y Estado de Derecho se cuenta.

Por lo que, se encuentra en nuestra realidad como nación, situaciones de índole común en la que cualquier persona con acceso a dicha interconexión de redes que le permita adentrarse a una súper carretera de la información, o al internet, se ven expuestas y vulnerables a conductas realizadas, propagadas, incentivadas, ejecutadas, planeadas y de cualquier forma de materialización delictivas, en donde se aprecia que otro elemento relevante dentro de las sociedades de la información como las redes sociales tienen un papel importantísimo, ya que a la falta de cultura de la legalidad y a la poca o nula legislación sobre este tema, cualquier

persona le puede dar un uso desde moralmente reprochable, hasta delincuencial a una red social, todo lo anterior responde a un tema de intercambio de información.

Hablando de la internet oscura *("Deep web o Darknet")* se hace notar que las disposiciones locales e internacionales simplemente se ven incapacitadas para evitar que se sigan ejecutando los actos terribles que se encuentran en ese mundo poco conocido y por ende, nulamente legislado y regulado del mundo de la interconectividad de la información.

Es conocido, por los medios masivos de comunicación y por las redes sociales, que simplemente en nuestro país, han ocurrido casos trágicos que lejos de ser moralmente reprochables, por contener material que atentan contra la dignidad de las personas, hay otros tantos que además de atentar de igual forma contra la dignidad de las personas, se convierten en conductas delictivas que incluso tienen desenlaces fatales ya que las instituciones de procuración, administración e impartición de justicia, así como sus respectivos operadores jurídicos se ven incapacitados para hacer frente a esta situación.

Desde el personal ministerial que sigue lidiando, a pesar de la implementación del sistema adversarial acusatorio, con los conocidos lastres *"jurídicos"* donde prefieren darle una explicación o solución al denunciante o víctima del delito que escapa totalmente de lo ocurrido en la verdad histórica del hecho, desde situaciones penosamente comunes, por ejemplo, a nivel educativo básico del acoso escolar que puede derivar en conductas delictivas o que bajo el ahora conocido *"bullying"* se encuentra soslayada una conducta delictiva que se encuentra perfectamente contemplada por la legislación penal y que simplemente prefieren darle solución como una *"constancia de hechos"* o hasta la nula regulación y por ende, una nula penalidad e imposición de sanciones penales para evitar la proliferación, elaboración, distribución y ejecución del material multimedia conocido como *"videos snuff"* donde se elaboran grabaciones de homicidios, secuestros, tortura, violaciones, necrofilia con el único fin de comercializar con

dicho material para entretenimiento que se desarrolla bajo la impunidad por falta de conocimiento, legislación y regulación de la interconectividad de redes e intercambio de la información, así como de una comprensión total de lo que implica una sociedad de la información.

Es conocido que en aras de la sociedad de la información en la que nos desenvolvemos, la "*Jurismática"* tiene cabida y comienza a desarrollarse en otras áreas del Derecho, como el Derecho Mercantil y los juicios en línea o la firma electrónica, que sin duda es una clara manifestación de la voluntad que hace diez años simplemente era inexistente, sin embargo, en materia penal, la "*Jurismática"* tiene presencia en etapa de investigación y en la etapa procesal como medios aportados por los avances científicos, sin embargo, como se describe líneas anteriormente escritas, no existe la aplicación del *"Ius Puniendi"* a conductas claramente delictivas, ni mucho menos acciones que sean contundentemente preventivas.

Mientras no exista una implementación total como política de Estado de una cultura de la legalidad y las instituciones del Estado, incluyendo la Constitución Política de los Estados Unidos Mexicanos ampliada, no preserven, fomenten y fortalezcan el Estado de Derecho y se permita que la "Jurismática" tenga desarrollo transversal en todas las áreas del Derecho, nuestro sistema jurídico estará lejos de atacar todas las atrocidades encontradas en el intercambio de información y material multimedia que claramente afectan los Derechos Humanos de las víctimas.

El presente trabajo de investigación se encuentra elaborado con el método analítico y el método deductivo, en virtud de que el problema planteado anteriormente será analizado en cada una de sus partes para su mejor entendimiento y solución y por otra parte será abordado en su aspecto general, como un todo, para llegar a una solución o propuesta de solución, que consiste en la elaboración multidisciplinaria de un artículo del Código Penal Federal, para su

creación en los diversos cuerpos normativos penales a nivel local, que contemple lo anteriormente descrito con todos y cada uno de los elementos que integran el delito para combatir de manera efectiva esta conducta que claramente viola o transgrede la dignidad humana, los Derechos Humanos, así como la elaboración de un eje temático que puede servir para las instituciones de procuración y administración de justicia para aplicar de manera efectiva acciones preventivas y de investigación que eviten la impunidad en este delicado tema.

En el presente trabajo también serán analizados las diversas disposiciones locales e internacionales respecto al objeto del presente trabajo, así como criterios de Nuestro Máximo Tribunal para proponer una línea de trabajo donde puede tener mayor desarrollo e impacto la “Jurismática”, así mismo la relevancia del planteamiento del problema responde a la creciente necesidad de rescatar y fortalecer el Estado de Derecho, a través, de instituciones capaces de salvaguardar y proteger el valor supremo de las personas, la Dignidad Humana y los Derechos Humanos.

CAPÍTULO I.

BREVE HISTORIA DEL INTERNET MUNDIAL Y EN MÉXICO.

1.1 HISTORIA DE INTERNET EN EL MUNDO.

Para hablar acerca de cómo el mundo conoció al Internet, es necesario remontarnos al año de 1969 del siglo pasado, en donde el producto de un experimento del Departamento de Defensa de los Estados Unidos llamado *"ARPANET"* donde intercambiaban información las principales universidades de aquel país, así como el personal militar de dicha Secretaría de Estado.[1]

Siendo así, que posterior a la creación de *"ARPANET",* se pensó en conectar esta nueva red a otras también gestionadas por el Departamento de Defensa de los Estados Unidos, siendo las candidatas para esta acción las redes *"PRNET"* y *"SATNET",* por lo que se da nacimiento al concepto de red de redes.

Debe entenderse que la red de redes, es una súper carretera de la información, que permite que cualquier computadora, se conecte a otras, sin limitación de ningún tipo, y así intercambien cualquier tipo de material multimedia.

Ahora bien, en el año de 1973, en la Universidad de Stanford, se logra que la nueva red de redes tenga un Protocolo de Control de Transmisión, denominado "*TCP"* por sus siglas en inglés, en el cual serviría de manual para regular la información controlada así como los usuarios que la comparten.

En este orden de ideas, en 1978, en la Universidad del Sur de California, dividen el TCP en dos partes para agregar el conocido protocolo interredes *"IP"* por sus siglas en inglés, creando así el TCP/IP, base en la cual hoy en día opera el Internet.

En 1983, el Departamento de Defensa de los Estados Unidos, crea la red "*MILNET"*, ya que estaba preocupado que por el creciente intercambio de

[1] Guazmayan Ruiz, Carlos. Internet y la Investigación Científica. El uso de los medios y las nuevas tecnologías en la educación. Alma Mater Magisterio. Página 21. Primera Edición 2004.

información, y por los pequeños avances de regulación del tráfico de estos datos, fueran vulnerables a un ataque por parte de alguna nación extranjera p alguna persona con fines perversos.

Recordemos que todo lo anteriormente narrado, es durante el contexto del periodo histórico-social conocido como *"Guerra Fría"* por lo que la preocupación extremista era cosa habitual en la época.[2]

Por lo que *"ARPANET"* se convirtió en *"ARPA-INTERNET"* y se le dio prioridad a los fines de investigación.

Ahora bien, en 1984, la Fundación Nacional para la Ciencia, en Estados Unidos, creo *"NSFNET"* siendo su principal red de intercambio de datos, siendo claro que cada vez más instituciones dedicadas a la creación y divulgación científica empezaban a utilizar la red de redes para sus funciones primarias.

La nueva red *"NSFNET"* utilizó *"ARPANET"*, por lo que de manera oficial, todo el intercambio de información y material multimedia, consistente en videos, audio, imágenes y texto, era intercambiado sin ninguna limitación por medio de las computadoras de Estados Unidos y el resto del mundo.

Derivado del trabajo constante de dicho experimento, en el año de 1990 se crea la conocida *"WORLD WIDE WEB"* donde se puede traducir como un conjunto de servidores de información multimedia conectados a la Internet.[3]

Siendo preciso aclarar que Internet no se limita únicamente a la *"WORLD WIDE WEB"*, también llamada *"WWW",* en virtud de que este servicio de intercambio de información solamente es el más conocido por la posibilidad de utilizar material multimedia (documentos, textos, videos, imágenes, audio, etc.).

---

[2] Heffer, Jean. Launay, Michael. La Guerra Fría 1945-1972. Ediciones Akal, S.A. 1992, página 25.

[3] Ovilla Bueno, Rocío. Boletín Mexicano de Derecho Comparado número 92. Internet y Derecho. De la realidad virtual a la realidad jurídica páginas 421-423. Instituto de Investigaciones Jurídicas. Primera edición 1998. México.

Ya que la capacidad de utilizar la Internet, es prácticamente infinita, tenemos por ejemplo, dejando de lado la llamada *"WWW"*, la capacidad de intercambiar mensajes de correo electrónico (*"e-mail"*) siendo este el segundo uso más conocido que se tiene para el Internet.[4]

Cabe precisar que para el año de 1995, existían 16 millones de personas en el mundo conectadas a la súper carretera de la información, utilizando el servicio *"WWW",* sin embargo, se cerró "*NSFNET"* para dar paso a los proveedores de Internet privados, así como al uso privado del mismo.

Lo que significaba que cualquier persona que pudiera comprar una computadora, esta ya vendría predeterminada de fábrica, para poder conectarse a la Internet, utilizando la *"WORLD WIDE WEB"* sin necesidad de acudir a alguna dependencia gubernamental ni mucho menos de contar con algún permiso.

Cabe precisar que en el año de 1977, en la Universidad de Chicago, se creó un programa al que denominaron *"MODEM",* el cual permitía el intercambio sin limitaciones de información entre diversas *"CPU".*

Por lo que en 1983, siendo ya público lo mencionado anteriormente, en California se crea un programa llamado *"BBS FIDONET"* que consistía en utilizar el intercambio de información logrado en 1977 con el proyecto *"MODEM"* pero ahora sería mucho más barato, pues se conectaría con la red telefónica del usuario.[5]

Por lo que esto, supuso de inmediato una conectividad de tres millones de personas de manera casi instantánea a la ya conocida súper carretera de la información.

[4] http://conceptodefinicion.de/internet/

[5] Guazmayan Ruiz, Carlos. Internet y la Investigación Científica. El uso de los medios y las nuevas tecnologías en la educación. Alma Mater Magisterio. Página 23. Primera Edición 2004.

En este orden ideas, es preciso mencionar que después de que el Internet era utilizado ya de manera comercial en los Estados Unidos, dejando de ser exclusivo del área militar, existieron diversos inconvenientes en aquella época que prevalecen en la actualidad o fueron base para los actuales, motivo del presente trabajo.

Basta mencionar que en el año 1981, en la Universidad de la Ciudad de Nueva York y en la Universidad de Yale, de manera conjunta, se crea la red *"IBM"* conocida como *"BITNET"* y esta era destinada para conectar de manera automática a todos los usuarios universitarios de todo Estados Unidos.

Si bien es cierto, el uso de la red *"BITNET"* supondría una prometedora forma de intercambio de información y conocimiento, así como su respectiva divulgación, entre el sector universitario comenzó la discusión acerca de la autoría de dicha red.

Por lo que se dio nacimiento al *"movimiento de fuente abierta"* conocido como *"movimiento de software abierto"*, que consistía en permitir el libre acceso a toda la información existente acerca de los *"software".*

Por lo que a raíz del *"movimiento de software abierto"* se crea una cultura de la información, donde las personas no solo querían acceder al conocimiento existente, también querían saber cómo crear conocimiento, liberar el que estuviera restringido a la opinión pública y divulgar el mismo a todos los usuarios de Internet sin ninguna limitación, por lo que aparece por primera vez, el concepto de *"hacker"*.[6]

En 1991, en la Universidad de Helsinki, Linus Torvalds, quien era estudiante de dicha Universidad, desarrolló un nuevo sistema operativo o *"software"* al que denominó *"LINUX"* publicándolo gratis en Internet, pidiendo a los internautas

[6] Guazmayan Ruiz, Carlos. Internet y la Investigación Científica. El uso de los medios y las nuevas tecnologías en la educación. Alma Mater Magisterio. Página 25. Primera Edición 2004.

que lo mejoraran si así lo consideraban y que igualmente lo compartieran de manera gratuita en la red.

Consecuencia de lo anterior, se considera en la actualidad a *"LINUX"* como el sistema operativo más avanzado, gracias a los complementos que millones de *"hackers"* han realizado.

Gracias a que en 1990, se creó la *"WWW"*, Internet ya no era exclusivo de usuarios universitarios de Estados Unidos, o del sector intelectual de aquel país, ya era propiedad de la humanidad, Internet ya era perfectamente accesible para cualquier persona con computadora en cualquier punto del planeta.

1.2 HISTORIA DE INTERNET EN MÉXICO.

En nuestro país, la historia del Internet es muy particular, luego de que en el año de 1982, el Departamento de Computación del Instituto de Investigación en Matemáticas Aplicadas y Sistemas por medio de su propia red llamada "*TELEPAC"* había podido conectarse a la red *"ARPANET",* siendo Max Díaz el primer investigador que intercambiaba información y datos por medio de dicha red.

Posteriormente en el año de 1987, en el Instituto Tecnológico y de Estudios Superiores de Monterrey, logró conectarse a la red "BITNET", aquella red descrita en el número anterior de este capítulo como la red que permitiría conectar a todos los universitarios de Estados Unidos.

En ese mismo año, la Universidad Nacional Autónoma de México, logra conectarse también a la red *"BITNET"* por medio de la conexión lograda por parte del Instituto Tecnológico y de Estudios Superiores de Monterrey.

Siendo así que en el año de 1988, la Universidad Nacional Autónoma de México y el Instituto Tecnológico y de Estudios Superiores de Monterrey firmán un acuerdo con la Administración Nacional de la Aeronáutica y del Espacio, mejor conocida como *"NASA"* por sus siglas en inglés y con la Fundación Nacional para la Ciencia en Estados Unidos, para intercambiar información especializada, teniendo dos enlaces aquí en México, uno en la UNAM en el campus de Ciudad Universitaria y el otro en el ITESM en el campus del Estado de México.[7]

Gracias a lo anterior, en el año 1989, la UNAM, logra la primera conexión a Internet de México, conectándose con la NASA y con la Fundación Nacional para la Ciencia en Estados Unidos, logrando el enlace gracias al satélite mexicano *"Morelos I",* se comunicaron usando TCP/IP, recordando que se

[7] Koenigsberger, Gloria. Los Inicios del Internet en México. 2014.

explicó y documento en el número anterior del presente capítulo, que TCP/IP es una forma de incluir un control en el tráfico de datos, teniendo orden en el material intercambiado así como en las computadoras involucradas, por lo que producto de lo anterior, se logró tener la primera dirección IP en nuestro país, siendo la denominada *"alfa.astroscu.unam.mx".*

Posteriormente se fueron involucrando diversas Universidades a la conexión a Internet, siendo que en el año de 1993, también logran conectarse a Internet el Consejo Nacional de Ciencia y Tecnología, la Universidad Autónoma Metropolitana y el Instituto Autónomo de México.[8]

Derivado de lo anterior, en 1995, Instituto Tecnológico y de Estudios Superiores de Monterrey crea el Centro de Información de Redes de México, quien es el encargado de darle el dominio "*.mx"* a todas aquellas páginas creadas en nuestro país.

En el año de 1999 se crea la Asociación Mexicana de Internet, organismo creado para recabar datos cuantitativos y cualitativos respecto al uso que se le da en México al Internet, incluye a todas las empresas privadas que constituyen el avance sistemático del Internet en nuestro país.

En nuestro país, el crecimiento e involucramiento de Internet en la vida común de los mexicanos es cada vez más amplia, hoy en día, gracias a la aparición de teléfonos inteligentes, algunos con modalidades de pagos o a bajo costo, permiten que la gran mayoría de los mexicanos cuenten con acceso a Internet.[9]

Si bien es cierto, la historia del Internet en nuestro país ha sido limitada, pues prácticamente somos un país con pocos años conectados, también lo es, que

---

[8] Gayosso, Blanca. ¿Cómo se conectó México al Internet?. Revista UNAM. ¿Crecimiento de uno o de todos? http://www.revista.unam.mx/vol.4/num4/art7/ago_art7.pdf

[9] Instituto Nacional de Estadística y Geografía (México). Estadísticas sobre disponibilidad y uso de tecnología de la información y comunicación en los hogares. 2013. Página 42.

al principio la sociedad no estaba interesada ni informada acerca del uso y la practicidad del internet.

Más allá de las esferas académicas, a mediados de la década de los noventa del siglo pasado, la sociedad no entendía que ahora ya estábamos conectados con el mundo, con un mundo globalizado.

Por ejemplo, en opinión del Doctor Erik Sigfrido Huesca Morales, la sociedad no se vio interesada en la aparición del Internet, hasta que en el año 1994 el Secretario de Relaciones Exteriores José Ángel Gurría declaró que la guerra que se efectuaba en aquel entonces en el estado de Chiapas, a raíz, del levantamiento en armas del Ejercito Zapatista de Liberación Nacional, "era una guerra de papel y de internet"[10], fue ahí cuando la sociedad mexicana comenzó a mostrar cierta inquietud sobre que es el Internet y cuáles eran los beneficios inmediatos del mismo, así como el impacto directo y permanente en la humanidad.

Resulta claro que a partir del nuevo milenio, cuando la accesibilidad a nueva tecnología, por ejemplo, los teléfonos inteligentes a bajo costo, permiten que la conectividad y el acceso a Internet sea paulatinamente mayor en México.

Si bien es cierto, la mayoría de los mexicanos tenemos acceso a la súper carretera de la información, también es cierto que este acceso es de los más caros entre los países que integran la Organización para la Cooperación y el Desarrollo Económico[11] por lo que resulta menester que las políticas públicas del Estado sean encaminadas a facilitar de mayor manera el acceso a Internet, así como para prevenir y castigar los delitos que con motivo de su uso se deriven, motivo del presente trabajo.

---

[10] Rodríguez, Erika. Historia de Internet en México.
Entrevista a Doctor Erik Sigfrido Huesca Morales. Agencia Informativa CONACYT. 9 de junio del 2016. http://www.conacytprensa.mx/index.php/ciencia/humanidades/7839 -historia-de-internet-en-mexico-reportaje

[11] El Universal. 13 de agosto del 2009. Sección Tecnología. http://archivo.eluniversal.com.mx/articulos/55127.html

CAPÍTULO II.

MARCO CONCEPTUAL DEL DELITO Y LA INFORMÁTICA EN MÉXICO.

2.1 CONCEPTO DEL DELITO.

Acerca del delito, es menester conocer que el Derecho Penal, perteneciente al Derecho Público, contempla perfectamente la conducta del delito, en su parte sustantiva, es decir, en la parte del Derecho Penal Sustantivo, siendo que el hecho materializado, es tema del Derecho Penal Adjetivo.[12]

Ahora bien, el delito también puede ser entendido como una conducta típica, antijurídica y culpable presupuestada en una conducta reprochable por el Estado, por medio del Derecho Penal, para castigar dicha conducta que altera el orden social, afecta o pone en peligro un bien jurídicamente tutelado o violenta una disposición normativa.

Nuestro ordenamiento jurídico sustantivo local, contempla, diversos principios que deben ser observados al momento de apreciar la posible reprochabilidad de una conducta delictiva.

Encontramos los siguientes:[13]

- Principio de legalidad
- Principio de tipicidad y prohibición de aplicación retroactiva, analógica y por mayoría de razón
- Prohibición de responsabilidad objetiva,
- Principio del bien jurídico y la antijuricidad material,
- Principio de culpabilidad y
- Principio de jurisdiciccionalidad.

---

[12] Díaz-Aranda, Enrique. Lecciones de Derecho Penal para el Nuevo Sistema de Justicia en México. Instituto de Investigaciones Jurídicas 2015. Página 43.

[13] Código Penal del Distrito Federal, publicado en la Gaceta Oficial de la Federación el 16 de julio del 2002, por el entonces Jefe de Gobierno Andrés Manuel López Obrador. Libro Primero Disposiciones Generales. Título Preliminar de los principios y garantías penales.

Aunque también encontramos acepciones al respecto como que el delito es una conducta humana condicionada por el criterio ético de la clase que domina la sociedad. [14]

Cabe la observación de Castellanos Tena, quien define que delito proviene de la palabra *"deliquere"* que significa apartarse del camino.[15]

Ahora bien, los conceptos de delito a lo largo del siglo XVIII, XIX y XX se desarrollaron de notoria manera, siendo el caso que el concepto de delito se ha agrupado en varias definiciones, mismas que pueden ser las siguientes:

- Concepciones nominales o formales.

Estas establecen que el delito es una conducta humana que se opone a lo que la Ley manda bajo la amenaza constante de una pena o sanción.

Es decir, es la Ley quien decide que conductas son o no son delito.

Dentro de este grupo, encontramos concepciones jurídicas y filosóficas al respecto.

Dentro de las concepciones jurídicas, entre otras tantas, podemos señalar que el delito es un ente jurídico y no un fenómeno social, es un ente jurídico porque es una contradicción entre el hecho del hombre y la Ley, por lo que se considera una infracción, siendo su esencia la antijuricidad.[16]

Desde luego que la acepción jurídica actualmente no es aceptada, ya que el delito no es creado por la Ley, la Ley solo lo define, define el tipo.

---

[14] Machicado, J. Concepto del delito. La Paz, Bolivia. Apuntes Jurídicos. 2010.

[15] Castellanos Tena, Fernando. Lineamientos Elementales del Derecho Penal. Porrúa. México. 1986. Página 125.

[16] Terragni, Marco Antonio. Estudios sobre la parte general del Derecho Penal. Universidad Nacional del Litoral, Santa Fe, Argentina. 2000. Página 104.

Aunque también tenemos las concepciones filosóficas, donde por ejemplo, nos dice que el delito supone la aplicación de un mal contra el autor del delito, es decir, la pena era un mal.[17]

O también donde se establece que el Derecho Penal debía ser seguido por todos los seres inteligentes sin distinción.[18]

- Concepciones substanciales o materiales.

Estas consideraciones establecen requisitos previos para que una conducta humana sea considerada como delito, así pues, el delito es una conducta que forzosamente requiere una actuar típico, antijurídico, culpable y sancionado con una pena.

Dentro de este grupo de concepción, se tiene la concepción dogmática y la concepción sociológica del delito.

La concepción dogmática establece que el delito es la conducta que el delincuente vulnera, es decir, el supuesto hipotético o presupuesto de la norma jurídico-penal.

Siendo el caso que el supuesto hipotético es el *"deber ser"* y la norma jurídico-penal es *"el ser"*, en otras palabras, de acuerdo a este concepción, el delito es una acción u omisión voluntaria típicamente antijurídica y culpable.[19]

Entendamos entonces:

- Acción u omisión voluntaria.

Desde luego quedan descartadas las conductas que no sean con conducidas por la voluntad del agente, por ejemplo, el error invencible, acto reflejo (reacción a un estímulo) situaciones ajenas a lo patológico (sonambulismo, sueño).

---

[17] Kant, Immanuel. La Metafísica. Página 207.

[18] Pellegrino, Rossi. Lineamientos Elementales de Derecho Penal. Porrúa. 2001.

[19] Mayer Ernest, Max. Derecho Penal Parte General. Editorial B de F. 2007.

- Es un acto típico.

Para considerarse delito debe adecuarse al tipo penal, si no hay tipo penal, no hay delito.

- Acto típicamente antijurídico.

El delito está en contra de la norma jurídica.

Sin embargo, una conducta así puede dejar de ser delito si intervienen Causas de Justificación de la acción, como por ejemplo:

- Estado de Necesidad.
- Ejercicio de un Derecho o Deber.
- Cumplimiento de una Ley o un deber.

También son conocidas como Causas de Exclusión del Injusto Penal, se interpreta como situaciones en las cuales la Ley Penal elimina la antijuricidad de una conducta descrita como delito para que la considere ahora como lícita, y por ende, sin delito.[20]

Ahora bien, el delito, dentro de esta visión, contempla el elemento de culpa, y para que la culpa pueda integrarse, debe contener los siguientes rubros:

- Imputabilidad.
- Dolo o culpa.
- Exigibilidad de un comportamiento distinto.

Sin embargo, la conducta deja de ser culpable cuando median causas de inculpabilidad como:

- Caso Fortuito.

[20] Mayer Ernest, Max. Derecho Penal Parte General. Editorial B de F. 2007.

- Cumplimiento de un deber o estado de necesidad.

Por último, dentro de esta concepción se aprecia la punibilidad, que se traduce como la sanción o castigo por la conducta reprochable por la Ley Penal, es decir, la privación lícita de un bien jurídico a quien haya cometido o intentó cometer un delito.[21]

Existen situaciones conocidas como Causas de Impunidad, que se traducen en circunstancias personales por las que a pesar de existir todos los elementos previos del delito, no se le puede aplicar sanción al delincuente, puede ser una medida de seguridad únicamente.[22]

Dentro de la concepción sociológica, se entiende que delito es la lesión de los sentimientos altruistas fundamentales de piedad y probidad en la medida media en que son poseídos por la comunidad y en la medida en la cual son indispensables por el individuo para su adaptación en sociedad.[23]

Ahora bien, por último, nuestro Ordenamiento Jurídico Penal Federal, reza en su numeral séptimo que delito es el acto u omisión que sancionan las Leyes Penales.

Mientras tanto, como lo mencione anteriormente, nuestro Ordenamiento Jurídico Penal Local, en su numeral quince, reza que delito solo puede ser realizado por acción u omisión, entendiendo que deben mediar los puntos señalados al principio de este número.

---

[21] Ibídem.

[22] Muñoz Conde, Francisco. García Aran, Mercedes. Derecho Penal, Parte General. Valencia, España. Tirant Lo Blanch. 2004. Página 405-406.

[23] Garofalo, Rafael. Indemnización a las víctimas del delito: Traducción y Estudio Crítico. Analecta. 2002. Página 172.

2.2 TEORÍA DEL DELITO.

Primeramente debemos entender como Teoría del Delito, como el conjunto de supuestos necesarios para poder entender una conducta como delictiva, esto significa que forzosamente requerimos conocer si todos y cada uno de dichos elementos que median el actuar de una persona por sí misma o por medio de otros mecanismos son considerados delitos.[24]

Los elementos a los que nos referimos, requieren de algunos ya explicados en el numeral anterior, dentro de la concepción substancial de delito, como la voluntad.

Sin embargo, existen otros elementos, más contemporáneos que requieren previo análisis, como el Nexo Causal.

También, para el estudio de la Teoría del Delito, debemos entenderá los elementos personales que en ella actúan, tales como el sujeto pasivo, activo y objeto del delito, es decir, en el bien jurídicamente tutelado por la Ley Penal.

Al momento de estudiar este concepto, podemos señalar dos teorías:

- Teoría Causalista del delito.
- Teoría Finalista del delito.

Para entender el primer precepto, en donde el máximo exponente es Franz Von Liszt, también conocida como Escuela Clásica del Delito, señalamos que la acción, es un movimiento cuya consecuencia ya está contemplada por la Ley Penal, entonces es irrelevante conocer la finalidad que originó la acción.

Por otro lado, la Teoría Finalista nace con Hans Welzel, esta teoría manifiesta que toda conducta humana tiene su origen en una acción regida por la voluntad, por lo

[24] Muñoz Conde, Francisco y García Arán, Mercedes, Derecho Penal. Parte General, Tirant lo blanch Valencia, 2002, p. 203.

que para poder analizar si dicha conducta constituye un delito, debemos atender a la voluntad del sujeto.[25]

Ahora bien, también existe la Teoría del Funcionalismo, su máximo exponente es Claus Roxin, quien establece que se reconoce los elementos del delito propuestos por el finalismo, pero con una orientación político-criminal, pues debe ser guiado por los fines del Derecho Penal.[26]

Una de las características de la teoría del delito son las siguientes:[27]

- Es un sistema porque representa un conjunto ordenado de conocimientos.

- Son hipótesis, pues son enunciados que pueden probarse, atestiguarse o confirmarse solo indirectamente, a través de sus consecuencias.[28]

- Posee tendencia dogmática al ser parte de una ciencia social. No existe unidad respecto de la postura con que debe abordarse el fenómeno del delito, por lo que existe más de un sistema que trata de explicarlo.

- Consecuencia jurídica penal: el objeto de estudio de la teoría del delito es todo aquello que da lugar a la aplicación de una pena o medida de seguridad.

Ahora, hablando de la Teoría del Delito, es vital entender la clasificación del mismo, por lo que atendemos a la siguiente clasificación del delito:

---

[25] Welzel, Hans, Estudios de derecho penal. Estudios sobre el sistema de derecho penal. Causalidad y acción. Derecho penal y Filosofía, Editorial B de F. Montevideo-Buenos Aires. 2003

[26] Roxin, Claus, Derecho penal. Parte general. Fundamentos. La estructura de la teoría del delito, trad. de Diego Manuel Luzón Peña, Miguel Días y García Conlledo, y Javier de Vicente Remesal, 2ª ed., Civitas, Madrid. 1997.

[27] Zaffaroni, Eugenio Raúl. Manual de derecho Penal. Parte General. 4ª reimpresión de la 2ª edición. Cárdenas, México D.F., 1998, Página 18.

[28] Bacigalupo, Enrique,. Lineamientos de la teoría del delito. Juricentro, San José, 1985, Página 143.

- Por su conducta (acción-omisión).
- Por el resultado (formales-materiales).
- Por su duración (Instantáneos-Permanentes-Continuados).[29]
- Por su persecución (Oficio-Querella).

[29] Código Penal del Distrito Federal, publicado en la Gaceta Oficial de la Federación el 16 de julio del 2002, por el entonces Jefe de Gobierno Andrés Manuel López Obrador. Título Segundo El Delito. Capitulo I. Formas de Comisión. Artículo 17.

2.3 ELEMENTOS DEL DELITO

El delito tiene diversos elementos que conforman un todo, estos elementos son la acción típica, antijurídica, culpable y punible, sometida a una sanción, desde luego penal.

El análisis de los mismos, permite conocer si existe o no delito.

Podemos apreciar los siguientes tres elementos, además de los ya mencionados anteriormente:

- Elemento genérico

Base sobre la cual se construye el concepto de delito.

- Elemento específico.

Permite diferenciar delito por delito, aunque no son constantes.

- Elemento Circunstancial.

Se refiere a la penalidad, es decir, al resultado del acto jurídico.

Dentro de los elementos del delito, encontramos los elementos positivos con su acepción negativa.

Conducta.	Ausencia de Conducta.
Tipicidad.	Atipicidad.
Antijuricidad.	Causas de Justificación.
Imputabilidad.	Inimputabilidad.
Culpabilidad.	Inculpabilidad.
Condicionalidad objetiva.	Falta de condiciones objetivas.
Punibilidad.	Excusas absolutorias.

2.4 ELEMENTOS POSITIVOS.

Dentro del rubro de elementos positivos del delito encontramos:

- Conducta.

Entendiendo que la conducta puede ser una acción o una omisión.

- Tipicidad.

Refiriéndonos a la adecuación de la conducta a lo presupuestado por el tipo penal.

- Antijuricidad.

Desde luego, es apreciable a lo que es contario por lo ordenado en la normal.

- Imputabilidad.

Aduciendo que el sujeto activo sea responsable del hecho delictuoso.

- Condicionalidad Objetiva de punibilidad.

Cuando al definir la infracción punible, aparecen variables de acuerdo a cada tipo penal.

- Punibilidad.

Lo relativo a la sanción por la conducta delictiva.

2.5 ELEMENTOS NEGATIVOS.

Dentro de este supuesto encontramos:

- Ausencia de conducta:

Realizar una conducta sin estar consciente de que se hace.

- Causas de Justificación:

Cuando se cuenta con un permiso para actuar respecto a la conducta delictiva.

- Atipicidad:

Desde luego es una falta de adecuación en la conducta del tipo penal.

- Inimputabilidad.

Cuando no se puede ser responsable de los hechos delictuosos.

- Inculpabilidad.

Cuando se destruye tanto el dolo como la culpa, no habiendo delito al respecto.

- Falta de condiciones objetivas de la punibilidad:

Cuando no aparecen todas las variables que dispone el tipo penal.

- Excusa absolutoria.

Se presupuesta un supuesto para que no exista castigo.

.

CAPÍTULO III.

REFERENTE A LOS ELEMENTOS DEL DELITO

3.1 RELATIVO A LA CONDUCTA Y SU AUSENCIA.

Respecto a este elemento del delito, que termina siendo un elemento básico para que pueda existir un delito en cuestión, se aprecia que la conducta puede desprenderse en dos supuestos: acción u omisión.

Ahora, entendiendo que existe diversidad de criterios para clasificar a este elemento, procedemos a su enunciado:

A) De resultado y de mera actividad.

Entendiéndose a las conductas consumadas, destacando que algunas conductas requieren solamente la actividad, mientras que otras requieren un resultado.

B) Instantánea y permanente.

De conformidad con nuestro Código Penal Federal, la conducta puede ser instantánea en virtud de que la lesión de un bien jurídicamente tutelado se puede realizar en un solo momento y nunca prolongarse en el tiempo.[30]

Sin embargo, la permanente se refiere a que la lesión del bien jurídicamente tutelado se prolonga en el tiempo, como por ejemplo, sucede en el delito de privación ilegal de la libertad.

C) De acción u omisión.

Entendemos que la mayoría de los delitos contemplados en nuestro ordenamiento jurídico penal federal, se refiere a conductas de acción, siendo muy claro en qué momento se materializa la conducta.

En cambio, la omisión aparece en contados tipos penales de nuestro Código Penal Federal, como por ejemplo, el abandono de personas. [31]

[30] Código Penal Federal. Artículo 7.
[31] Código Penal Federal. Artículo 340.

D) dolosa y Culposa.

En la conducta solo se permiten dos forma de comisión, dolo o culpa, quedando ya fuera de uso o excluida la forma llamada preterintencional de nuestro Código Penal Federal.

Podemos determinar que el dolo existe cuando el sujeto activo conoce y quiere las consecuencias de su actuar, realizándolo de esta manera.

En cambio, la culpa surge cuando el activo no tiene intención o no conoce las consecuencias o no tomó las medidas de cuidado suficientes y se produjo la conducta delictiva en cuestión.

E) De lesión y de peligro.

El primer supuesto requiere que un delito en cuestión, lesione un bien jurídicamente tutelado, para considerarse como un hecho consumado.

Sin embargo, el supuesto de puesta en peligro, requiere únicamente que se amenace intensamente al bien jurídicamente tutelado para que se materialice el delito a tratar.

F) Comunes y Especiales.

Dentro de las comunes, encontramos cuando el sujeto activo de determinada conducta delictiva puede ser cualquier persona que se encuentre en el supuesto que contempla la norma penal.

Sin embargo, el segundo supuesto, requiere que el sujeto activo, para poder ser reprochado por su actuar delictivo en determinado tipo penal, tenga una calidad especial.

Señalando las conductas especiales propias e impropias, puntualizando que las primeras se refieren a que determinada conducta solo será considerada delito cuando el sujeto activo tiene la calidad requerida en el tipo penal.

Por lo que la conducta típica especial impropia se refiere a que esta conducta está prevista en dos tipos penales con diferentes rubros, solo que se diferencian en que en uno requiere la calidad especial el sujeto activo y en el otro, puede ser cualquier persona el autor del delito.

Ahora bien, la conducta se integra con los elementos de:

- Objetivos.
- Normativos.
- Subjetivos.

Precisando que analizando cada uno de los elementos entenderemos si la conducta en cuestión es típica o no lo es.

Por lo que resulta de vital importancia el análisis de estos elementos, porque por ejemplo, en los delitos que requieren una acción para su materialización, encontraremos que tendrá mayor preponderancia los elementos objetivos, sin embargo, en los delitos por omisión, encontraremos que el elemento normativo tendrá mayor presencia.

Hablando de los elementos objetivos, precisamos que es el más importante para determinar que existe o no un delito, pues la conducta prohibida está contemplada por el cuerpo normativo.

El elemento objetivo, tiene dos elementos, mismos que señalamos:

- Voluntad.
- Nexo Causal.

Siendo que el primero se refiere a que la conducta, para ser considerada delito, debe ser voluntad del activo realizarla, en todo momento el sujeto pudiendo controlar su cuerpo, optó por realizar la conducta.

Ahora bien, respecto al segundo elemento, nos referimos a que la conducta que desplegó el activo, desencadeno una serie de resultados que son atribuibles a la conducta contemplada como tipo penal.

Ahora hablando de los elementos normativos, señalamos que se refieren a los que requieren una valoración cultural o jurídica para su existencia.

Dentro del rubro de lo cultural encontramos los conocidos elementos normativos culturales, donde para poder determinar si una conducta que sí está contemplada en el ordenamiento jurídico es delito, se necesita valorar si el contexto de la sociedad así lo aprecia, pues, pueden existir condiciones donde no se consideraría delito en virtud de ser socialmente aceptadas.

En cambio, en el rubro de la valoración jurídica, o conocidos como elementos normativos jurídicos, se clasifican en expresos e implícitos.

Refiriéndonos que los expresos son las descripciones de tipos penales que su redacción o las palabras que ahí se encuentran, nos remiten a diversos cuerpos normativos para su mayor comprensión.

Siendo el caso que los implícitos, se dirigen para entender hasta dónde puede llegar el alcance de la prohibición contemplada en la norma penal.

Ahora, refiriéndonos a los elementos subjetivos, encontramos que se dirigirán para tratar de explicar la conducta desplegada por el actor, es decir, la finalidad.

En atención a nuestro Código Penal Federal, sabemos que las acciones u omisiones solo se pueden realizar de manera dolosa o culposa, sin embargo esta disposición, se debe entender como elemento subjetivo genérico.

Pero también existen los elementos subjetivos específicos, siendo que se refieren a cuando el tipo penal establece la concurrencia de un determinado ánimo, fin o propósito.

Es preciso señalar que son muy pocos los delitos que requieren el elemento subjetivo específico para su existencia.[32]

Ahora hablando del elemento subjetivo genérico, de nueva cuenta, encontramos al dolo, aunque existen tres tipos, dolo directo, indirecto y eventual.

Nos referiremos al dolo directo, siendo que se dirige para explicar qué obra con este elemento quien tiene la intención o propósito del autor.

Es decir, obra con dolo directo, quien quiere realizar una conducta con el único objetivo de realizar un resultado específico "*exante"* y consigue el fin perseguido "*expost"* [33]

Ahora, el dolo indirecto, se refiere a que el sujeto quiere realizar una conducta con un fin que quiere alcanzar, pero para conseguirlo necesita realizar otros resultados que no quiere pero los acepta y sigue con su actuar, por lo que también se le llama dolo de consecuencias necesarias.[34]

Acerca del dolo eventual, el sujeto sabe lo que ocurre a su alrededor y quiere realizar una conducta que seguramente producirá un resultado que no quiere pero se muestre aquiescente, es decir, no hay certeza pero es muy probable que ocurra.

Hablando de la culpa, nos referimos a que de acuerdo al Código Penal Federal, dice:

> *Artículo 9o.- Obra dolosamente el que, conociendo los elementos del tipo penal, o previendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley, y Obra culposamente el que produce el resultado típico, que no previó siendo previsible o previó confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales.*

---

[32] Díaz-Aranda, Enrique. Lecciones de Derecho Penal. Instituto de Investigaciones Jurídicas. 2015. Página 96.
[33] Ibídem. Página 108.
[34] Ibídem. Página 111.

Dicha regulación se basa en el aspecto subjetivo de no aceptar el resultado y otro de carácter normativo de no acatar un deber de cuidado.

Existe la culpa con representación, refiriéndose al nexo psicológico que une al autor con el resultado.

También existe la culpa sin representación, basada en el supuesto de que el sujeto actuó sin pensar en el posible resultado, pero siendo reprochable el contravenir la norma.

3.2 RELATIVO A LA TIPICIDAD Y LA ATIPICIDAD.

Sabiendo lo que dispone la tipicidad, conociendo a que se refiere y que es, dirigido a que entender el encuadramiento del presupuesto del tipo penal en el caso concreto, en virtud de lo anterior, procederemos a entender primeramente las causas de atipicidad.[35]

Primeramente por causas de atipicidad, entendamos que la conducta no es típica, es decir, es lícita, en virtud de que falta alguno de los elementos de la conducta.

Existe la exclusión del elemento objetivo, es decir, falta de acción y falta de nexo causal.

Por falta de acción, se refiere a que el delito no se da porque simplemente no existió la conducta o es anulada, aunque también quedaría anulado cuando existe ausencia de voluntad, es decir, el activo no tenía el dominio y control sobre su cuerpo.

Por lo que a su respecto, se identifica la fuerza física irresistible, misma que puede ser "*vis absoluta*" y "*vis mayor".*

La primera se refiere cuando una persona impone su fuerza física a otra, anulando su posibilidad de dominar su cuerpo, y por el segundo supuesto, entenderemos que se encuentra en presencia de una fuerza irresistible proveniente de la naturaleza, que impidió que el hombre controlara su movimiento o su cuerpo.

Ahora por falta de nexo causal, nos referimos a la ausencia de elementos normativos culturales requeridos por el tipo.

Ahora bien, la falta de resultado también excluye la conducta típica consumada, misma condición que se encuentra en la fracción II del Artículo 15 del Código Penal Federal.

---

[35] Ibídem. Página 129

3.3 ANTIJURICIDAD.

Al respecto, es necesario entender que solo después de haber comprobado que la conducta determinada es típica, entonces podremos entender si es contraria al orden jurídico.

Si después de dicho análisis, comprobamos que la conducta es típica y antijurídica, entonces estamos ante un también llamado injusto penal, pero si aparece una causa que justifique la conducta típica, entonces quedará excluida la conducta típica y por ende, su antijuricidad, por lo que de manera obvia resultara que no existe delito.

Algunos consideran a la tipicidad como el indicio de la antijuricidad, toda vez que la mayoría de las conductas solo en muy pocas ocasiones estarán amparas por una causa de justificación.[36]

Las causas de justificación cumplen una función político-criminal, pues el legislador al crearlas, intentó justificar las causas, que si bien es cierto, podrían ser consideradas como delito, excluyen esa conducta por existir alguna condición que la misma ley permite.

La antijuricidad tiene dos aspectos, uno formal y otro material, siendo el primero el relativo a que no solo contraviene el Derecho Penal, sino a todo el sistema jurídico en su conjunto, formalmente estamos ante un injusto.

Mientras que la antijuricidad en su aspecto material, se refiere a que la lesión o la puesta en peligro de un bien jurídicamente tutelado es aceptada por la sociedad si salvaguarda un bien mayor que la sociedad espera que no se vea afectado.

---

[36] Zaffaroni, Eugenio Raúl. Manual de Derecho Penal, La Mesa, México. Cárdenas Editor y Distribuidor. 1988. Página 511.

3.4 CAUSAS DE JUSTIFICACIÓN.

Al respecto cabe el análisis de que el Código Penal Federal, contempla como una causa de justificación, el consentimiento del sujeto pasivo, al respecto me permito transcribir:

> *Artículo 15.- El delito se excluye cuando:*
>
> *III.- Se actúe con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:*
>
> *a) Que el bien jurídico sea disponible;*
>
> *b) Que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo; y*
>
> *c) Que el consentimiento sea expreso o tácito y sin que medie algún vicio; o bien, que el hecho se realice en circunstancias tales que permitan fundadamente presumir que, de haberse consultado al titular, éste hubiese otorgado el mismo*

Cabe el análisis si el consentimiento, cuando el legislador lo contemplo, excluye el delito porque se le considera causa de exclusión de la tipicidad de la conducta o si bien, el delito queda excluido porque dicho consentimiento justifica la conducta del sujeto activo.[37]

Por lo que para responder a lo anterior, nos encontramos que el consentimiento tiene plena eficacia, porque el legislador tiene la intención de proteger, única y exclusivamente, la libre disposición del titular del bien jurídicamente tutelado.

Ahora, hablando de causas de justificación, nos encontramos ante la legítima defensa, está reconocida en la fracción IV del mismo numeral 15 del Código Penal Federal, que reza:

---

[37] Díaz-Aranda, Enrique. Lecciones de Derecho Penal. Instituto de Investigaciones Jurídicas. 2015. Página 156

Artículo 15.- El delito se excluye cuando

IV.- Se repela una agresión real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se defiende.

Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente, al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien, lo encuentre en alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión;

Cabe precisar que todas fracciones contempladas en el numeral 15 de nuestro Código Penal Federal, excluyen el delito como una última consecuencia.

Por lo que resulta que la legítima defensa es una conducta típica, pero justificada, por lo que se resuelve en la antijuricidad, y por consiguiente el delito queda excluido.

La legítima defensa tiene dos elementos fundamentales, la protección del derecho individual y la defensa del orden jurídico.

Al respecto el primer elemento, significa que la justificación por legítima defensa presupone siempre que la acción típica sea necesaria para impedir o repeler una agresión antijurídica a un bien individual.[38]

[38] Ibídem. Página 162.

Cabe destacar que se excluye a los bienes jurídicamente tutelados colectivos, en virtud de que esa función corresponde al Estado, para no entrar en conflicto con el numeral diecisiete Constitucional.

La legítima defensa tiene sus elementos consistentes en repeler, entendiéndose por rechazar una agresión, motivo por el cual solo justifica al agredido frente al sujeto activo.

Ahora bien, el otro elemento es la agresión, referida a una amenaza de un bien jurídico tutelado por una conducta humana.

Cabe señalar que el elemento real, se refiere a que dicha agresión sea verdaderamente tangible en el mundo real, por lo que no caben las suposiciones, por eso no contempla el legislador, la legítima defensa putativa.

Se necesita también que exista una amenaza actual o inminente, por lo que al usar estas palabras, el legislador inscribió la vigencia de la legítima defensa.

Se requiere así mismo, como elemento de la legítima defensa, el actuar sin derecho, pues se espera que provenga frente a una situación en la cual, si bien es cierto hay una afectación a un bien jurídicamente tutelado, también lo es que dicha afectación, está formada por el Derecho.

Ahora, en la legítima defensa, se requiere que quien se encuadre en es este supuesto, solo podrá hacerlo para proteger bienes propios o ajenos, por lo que volviendo a aclarar que la legítima defensa, no permite la defensa de bienes jurídicamente tutelados colectivos, pues esta es tara del Estado, quien en su Constitución Federal lo prohíbe.

Uno de los elementos de la legítima defensa, es el de la necesidad de defensa, refiriéndose cuando no hay ni9nguna autoridad del Estado que pueda resguardar el bien, pues de haberla, no estaría justificada la conducta.

En este orden de ideas, la proporcionalidad juega un papel importante, pues tiene la equivalencia de la agresión con la repula.

Y por último, la ausencia de provocación, es decir, quien acude a la figura de la legitima defensa, no podrá iniciarla si fue quien provocó la puesta en peligro o la lesión a su bien jurídicamente tutelado o el de un tercero.

El cumplimiento de un deber cabe en este apartado, pues, además de ser contemplado en el Código Penal Federal, es uno de los más controversiales, pues casi siempre e realizada por los cuerpos se seguridad pública al momento de realizar sus deberes, sin embargo, llegan a verse inmersos en temas de posible violación de Derechos Humanos, tema que no es motivo de análisis del presente trabajo.

Por ende, el cumplimiento de un deber, está condicionado a la existencia de ese deber presupuestado por una norma jurídica, eso nos lleva a la figura de obediencia jerárquica, en la cual el cumplimiento del deber solo será válido esta excluyente de delito, si la orden del superior era lícita.

3.5 CULPABILIDAD.

La culpabilidad se basa en la posibilidad de ser reprochada una conducta a quien la realizó o participó en su realización.

Para poder realizar el juicio de culpabilidad se requiere forzosamente todos los factores que previamente condicionaron al autor del hecho reprochable.

Por lo que el numeral 52 del Código Penal Federal establece:

> *Artículo 52.- El juez fijará las penas y medidas de seguridad que estime justas y procedentes dentro de los límites señalados para cada delito, con base en la gravedad del ilícito, la calidad y condición específica de la víctima u ofendido y el grado de culpabilidad del agente, teniendo en cuenta:*
>
> *I.- La magnitud del daño causado al bien jurídico o del peligro a que hubiere sido expuesto;*
>
> *II.- La naturaleza de la acción u omisión y de los medios empleados para ejecutarla;*
>
> *III.- Las circunstancias de tiempo, lugar, modo u ocasión del hecho realizado;*
>
> *IV.- La forma y grado de intervención del agente en la comisión del delito;*
>
> *V.- La edad, la educación, la ilustración, las costumbres, las condiciones sociales y económicas del sujeto, así como los motivos que lo impulsaron o determinaron a delinquir. Cuando el procesado perteneciere a algún pueblo o comunidad indígena, se tomarán en cuenta, además, sus usos y costumbres;*
>
> *VI.- El comportamiento posterior del acusado con relación al delito cometido; y*
>
> *VII.- Las demás condiciones especiales y personales en que se encontraba el agente en el momento de la comisión del delito, siempre y cuando sean relevantes para determinar la posibilidad de haber ajustado su conducta a las exigencias de la norma.*

Por lo que las fracciones V y VII ofrecen parámetros para realizar el juicio de culpabilidad en comento.

Para empezar, necesitamos conocer la imputabilidad, es necesario que quien comete el delito, tenga la capacidad psíquica de comprender lo que está cometiendo.

En nuestro país, como es sabido, se determinó que la mayoría de edad es a los dieciocho años de edad, no es objeto del presente trabajo de investigación precisar si es correcto o no, únicamente se aprecia para efectos de comprender el tema a tratar.

Por lo que es importante reconocer que la imputabilidad se fija en el momento de la comisión del delito, sin importar otro factor más.

Además de la mayoría de edad, en nuestro país, se requiere que dicho sujeto no este editado bajo la figura de la interdicción judicial, pues de lo contrario, no tendría pleno control de sus facultades mentales.

4.6 EXCLUYENTE DE CULPABILIDAD.

Al respecto cabe señalar, que la culpabilidad quedará excluida por inimputabilidad o por inexigibilidad de otra conducta en los supuestos de miedo grave, temor fundado, estado de necesidad exculpante, error sobre la justificación y error de prohibición.[39]

Se consideran inimputables a todas las personas que al momento de la comisión del delito tenían menos de dieciocho años de edad, es decir, eran interdictas naturales.

Sin embargo, los menores de edad, existen las medidas de seguridad, plenamente contemplada en nuestro marco normativo penal.

Existe también el trastorno mental, siempre que este sea permanente, podríamos estar ante una excluyente de culpabilidad, como la locura o el retraso mental.[40]

Dichas condiciones mentales impiden un reproche al sujeto activo, porque no tiene la capacidad mental para comprender la trascendencia e implicaciones de sus actos.

El miedo grave solo excluye la imputabilidad del sujeto cuando anulan por completo su capacidad de comprensión y fueron producto de causas ajenas a su comprensión.[41]

En el miedo grave, la afectación a la psique del autor al momento de realizar el delito es a tal grado que anula su capacidad de discernir si está bien o mal.

Quien tiene temor fundado, mantiene su capacidad para comprender las implicaciones del injusto, pero las circunstancias lo orillaron a cometerlo.[42]

---

[39] Ibídem. Página 217.
[40] Ibídem. Página 219.
[41] Ibídem. Página 220.

Al respecto, el estado de necesidad exculpante, está detallado en la fracción V del numeral 15 del Código de Penal Federal, el cual se presenta cuando hay un conflicto ente dos bienes del mismo valor y solo uno de ellos se puede salvar.[43]

El error de prohibición se da cuando el sujeto se equivoca al creer que su comportamiento es lícito, cuando en realidad está prohibido por el Derecho Penal.

El error de prohibición puede ser vencible cuando con un mínimo de cuidado el sujeto habría podido conocer la ilicitud de su proceder.

[42] Ibídem. Página 223.
[43] Ibídem. Página 225

CAPÍTULO IV.

REFERENTE A DELITOS INFORMÁTICOS.

4.1 DERECHO INFORMÁTICO.

El derecho Informático es una disciplina en continuo desarrollo, tiene diversos antecedentes históricos, entre los cuales, podemos señalar el año de 1949 la obra de Norbert Wiener[44] explicando la relación que la cibernética impone al Derecho.

Cabe ser preciso, en que esta antelación, se da en el marco de la llamada *"Guerra Fría"*, por lo que la imposición a la que el autor se refiere, se da en el área de comunicaciones.

Sin embargo, en ese mismo año, el Jurista estadounidense Lee Loevinger publicó en la revista *"Minnesota Law Review"* el artículo llamado *"The Next Step Forward"* en el que afirma que el gran paso del hombre debe ser el de la transición de la Teoría General del Derecho hacia la Jurimetría.[45]

Ahora bien, podríamos decir en un concepto que el Derecho Informático es la Técnica Interdisciplinaria que tiene por objeto el estudio y la investigación de los conocimientos de la informática general, aplicable a la recuperación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesaria para lograr dicha recuperación.[46]

Existen diferentes denominaciones al respecto, por ejemplo:

- Jurimetría.
- Juscibernética.[47]
- Jurismática.

---

[44] Wiener, Norbert. Cibernética y Sociedad. Capítulo IV. Derecho y Comunicaciones. FCE. México. 1980

[45] Loevinger, L. "The Next Step Forward" en Minessota Law Review, Vol. XXXIV, 1949. Página 455-493.

[46] Téllez Valdés, Julio. Derecho Informático. Cuarta Edición. Mc GrawHill. 2009. Página 10.

[47] Losano, M. Giuscibernética. 1960. Página 101.

Para establecer si el Derecho Informático es una rama del Derecho, se necesita saber si cuenta con los rubros necesarios de las ramas autónomas:[48]

- Existencia de una legislación específica.
- Estudio de la materia.
- Desarrollo de Investigaciones.
- Existencia de Instituciones Propias.

Para el Doctor Julio Téllez Valdez, el Derecho Informático se define como una rama de las ciencias jurídicas que considera a la Informática como instrumento (Informática Jurídica) y objeto de estudio (Derecho de la Informática).[49]

Resulta claro, que el Derecho Informático, en la actualidad ocupa un lugar preponderante, en virtud de que a pesar de que sus primeros conceptos se dan en la década de los cincuenta, la utilidad actual hace que sea un elemento indispensable para figuras que hace simplemente una década era impensable, por mencionar algunas, el comercio electrónico, la firma electrónica, los medios de prueba por avances tecnológicos, y resulta sorprendente el caso de la cibercorte en Michigan, Estados Unidos, donde en el año 2002 se implementó una corte donde las audiencias, las comparecencia, los alegatos, el ofrecimiento y desahogo de pruebas se da en línea, ninguna de las partes que intervienen están físicamente en el lugar, sin embargo, las resoluciones de dicha cibercorte, dan plena seguridad y certeza jurídica.[50]

---

[48] Hernández Hernández, Selene Guadalupe. Análisis Jurídico sobre la necesidad de crear un capítulo especial denominado delitos cometidos a través de la utilización de medios informáticos dentro del Código Penal para el Distrito Federal. México. Aragón. 2008.

[49] Téllez Valdés, Julio. Derecho Informático. 3ª edición, Editorial McGraw Hill. Serie Jurídica. México. 2003. Página 17.

[50] Téllez Valdés, Julio. Derecho Informático. Cuarta Edición. Mc GrawHill. 2009. Página 50.

Ahora bien, resulta claro que por lo anteriormente expuesto, el Derecho Informático, sí es considerado y debe seguir siéndolo una rama del Derecho, en virtud de que puede relacionarse íntimamente con otras ramas del Derecho, así como que existe legislación al respecto, si bien es cierto no es basta, es necesario comprender que se está explotando en el país apenas el concepto de Derecho Informático, además también existe investigaciones e instituciones específicas sobre esta poco conocida y explotada área del Derecho.

En este orden de ideas, con mayor razón se le debe dar una consideración de rama del Derecho, porque se relaciona con el Derecho Penal, específicamente en el área de delitos informáticos, mismos que a la luz de la Teoría del Delito pueden ser estudiadas dichas conductas, sin embargo, la particularidad de las mismas no siempre está contemplada por dicha legislación penal, por lo que se debe complementar y relacionar con el Derecho Informático para prevenir actos delictivos que ensanchen más la brecha de impunidad.

4.2 HARDWARE.

Para poder analizar y realizar el presente trabajo, además de obviamente entender a la luz del Derecho Penal y la Teoría del Delito, así como del Derecho Informático y sus respectivos delitos en esa área, debemos entender las partes que integran todo el complejo físico que componen una computadora, elemento sin el cual, difícilmente se puede hablar de Derecho Informático.

Consiste en *"Hardware"*:

- Unidad de entrada.
- Unidad de salida.
- Unidad de procesamiento.
- Memoria y dispositivos de almacenamiento.

Un elemento indispensable en el funcionamiento de una computadora y el procesamiento de datos es la memoria, existiendo dos tipos:

- Memoria RAM.
- Memoria ROM.

Siendo la primera el almacenamiento permanente de información, pero cuyo contenido es solo temporal, y el segundo supuesto se refiere a memoria de solo lectura, más pequeña que el procesador, que se encuentra debajo de la tapa del mismo.

4.3 SOFTWARE.

De la misma forma, es vital conocer que es el denominado *"software"*, siendo que se refiere al conjunto de programas, documentos y aplicaciones que integran el funcionamiento de una computadora.

Es decir, es complementario del *"hardware"* quien no podría realizar nada, si no hay un *"software"* que le indique específicamente que realizar.

El *"software"* permite que un programa cumpla satisfactoriamente sus funciones.

Ahora bien, resulta menester conocer los cuatro grupos en que se divide esta importante parte de la computadora:

- Sistema Operativo.

  Organiza todas las actividades de la computadora, así como el intercambio de información.

- Lenguaje de Programación.

  Consiste en el programa en el que se le indica que tarea y como realizar dicha tarea a la computadora.

- Software de uso general.

  Estructura de aplicaciones científicas, académicas y empresariales.

- Software de aplicación.

  Estructura de tareas más específicas, por ejemplo, permite que la computadora reconozca una memoria extraíble USB.

4.4 INTERNET OBSCURA.

Acerca del Internet, una vez explicado en la primera parte de este trabajo, el origen, la historia y el concepto, debemos ahora explicar y entender que es Internet Obscura.

Por Internet Obscura, también conocido como *"Darknet"* o *"Deepweb"* se entiende todo intercambio de información multimedia, igual que Internet convencional, solo que la diferencia soslaya en que las conexiones a Internet no se realizan por medio de los servidores que utiliza la Internet, si no que se realiza por *"nodos"* entendiéndose por *"nodo"*, como una red donde confluyen diferentes computadores para conectarse a Internet.

Ahora bien, estos *"nodos"* funcionan con servidores denominados *"proxys"* mismo que permiten cambiar constantemente, de manera virtual, la ubicación de la computadora, así como el usuario conectado a internet por medio de ella.

Gracias a los servidores *"proxys"* podemos encontrar en la Internet obscura, un sinnúmero de usuarios, que amparados en el anonimato, intercambian material multimedia que representan conductas delictivas, como por ejemplo, por mencionar algunas:

- Venta de sustancias psicotrópicas.
- Venta de armas.
- Servicios de sicariato.
- Intercambio de material pornográfico.
- Intercambio de material de pedofilia.
- Intercambio de material de zoofilia.
- Intercambio de material de necrofilia.
- Torturas.
- Mutilaciones.
- Maltrato Animal.

Dicho material, que claramente está contemplado como conductas delictivas por nuestros ordenamientos jurídicos penales federales y locales, son imposibles de perseguir, pues además de la naturaleza de la conexión que realizan, que permite virtualmente estar en diferentes partes del planeta al mismo tiempo, nuestro cuerpo normativo no cuenta con un tipo penal específico para estas conductas, atendiendo a la naturaleza de la conexión, la voluntad de intercambiar datos por medio del anonimato y las circunstancias concretas.

Si bien es cierto, existen diversos tipos penales que contemplan estas conductas, también lo es, que en materia procesal, no existen suficientes medios para perseguir a los sujetos activos de la mismas, además de que incluso en materia sustantiva no existe el tipo penal que regule la totalidad de las mismas, por ejemplo, si una persona sube a la Internet Obscura un video donde manifiesta que ofrece sus servicios para secuestrar a sueldo, y es conocidos por todos los usuarios de esa red que existe una posible conducta delictiva que se llevará a cabo de forma inminente, así como la identidad del sujeto activo e incluso la del pasivo, y pensando más allá, es conocido por todos ellos, el lugar donde el pasivo está privado de su libertad así como las constantes torturas e incluso muerte que se le dé….¿Acaso nuestro cuerpo normativo está rebasado por esta muestra cínica del delito? ¿Cómo se castiga si no existe un tipo penal que castigue anunciar que se va a secuestrar a alguien? Parece que debe revisarse entonces todos y cada uno de los elementos del tipo penal, los requisitos de procedibilidad e incluso las políticas públicas al respecto.

4.5 VIRUS INFORMÁTICO.

Por virus informático se entiende un programa relativo a la informática que tiende a alterar el funcionamiento de la computadora, generalmente para su detrimento, sin que el usuario se percate de ello.

Generalmente modifican los archivos de la computadora receptora, para que de forma intencionada, destruyan o modifiquen todo aquel documento que se encuentre almacenado en ella.

La forma más común en la que una computadora se infecta es por medio del uso de interfaces entre el *"hardware"* y el *"software",* por ejemplo, una entrada "*USB"* o por medio de discos compactos, así como también por enlaces maliciosos enviados por medio de redes sociales o por correo electrónico.

Los virus informáticos funcionan primeramente alojándose en una computadora receptora, posteriormente se instalan en la memoria "*RAM"* de la misma, para comenzar a afectar los archivos que se encuentren ahí.

Una vez realizado lo anterior, cuando la computadora es apagada por el momento, y en otro momento se pretende volver a utilizar y se enciende, el virus informático se reproduce tomando por completo el control de los archivos de la computadora, por lo que permite más fácil su reproducción, logrando con ello, poder infectar a otras computadoras que se conecten con la primera computadora receptora, por medio de correos electrónicos o por medio de las interfaces ya descritas anteriormente.

Existen diversos tipos de virus, tales como gusanos, troyanos, "*spyware",* por mencionar unos cuantos, que tienen características únicas o compartidas en ocasiones, y que afectan el funcionamiento de la computadora.

4.6 ANTIVIRUS Y OTRAS FORMAS DE PROTECCIÓN.

Un antivirus es un programa informático que tiene la principal función de localizar e impedir la intromisión de otros programas informáticos maliciosos en la computadora, que tienen la finalidad de alterar el funcionamiento de la misma en su perjuicio, se les conoce como virus.

Un programa de antivirus, funciona escaneando todos y cada uno de los archivos que el usuario de la computadora tenga almacenada en la misma, así como de todo aquel dispositivo ajeno a la computador que sea introducida a la misma, sin dejar de lado, todo aquel archivo que se descargue en la computadora.

El escaneo que el antivirus realiza, lo logra analizando cada archivo, ya sea descargado, enlazado a la computadora o ya almacenada en esta en su memoria, lo coteja con una lista ya conocida de virus informáticos y si encuentra alguno que se dé positivo en el cotejo, inmediatamente, impide que el virus informático se ejecute y procede a su eliminación.

También existen otras formas de protección informática, complementarias de un antivirus, conocidas como "*firewall"* y los *"antispyware",* entendiendo que un *"firewall"* es un dispositivo de seguridad conectado a la red que monitorea constantemente el tráfico de datos por internet, decidiendo si bloquea o no, algún dato que se quiera descargar o enlazar a nuestra computadora por medio de internet, este análisis para decidir si bloquea o no el contenido de algún dato de la red, lo hace de acuerdo a los estándares de reglas de seguridad informática.[51]

Un firewall puede ser, entre otros, *"firewall proxy", ""firewall de inspección activa"* y el *"firewall de próxima generación"* por mencionar algunos.

Los *"firewall"* pueden ser de *"hardware", "software"* o ambos.

[51] http://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

CAPITULO V.

DELITOS INFORMÁTICOS EN MÉXICO.

5.1 DELITOS INFORMÁTICOS.

En nuestro país, el conocimiento técnico-jurídico acerca de los delitos informáticos hasta hace poco era desconocido, nuestros ordenamientos legales sustantivos en materia penal, a nivel local y federal, no contemplaban dentro de su cuerpo normativo a cabalidad estas conductas.

Recientemente, el 28 de marzo del año 2012, nuestro Código Penal Federal fue modificado, en los numerales 211, 282, 389 y 390 con el fin de unificar conceptos y conductas de los delitos informáticos.

Resulta importante mencionar, que para el numeral 211, se le adiciona un capitulo nuevo, creando el artículo 211 bis, donde se sanciona el acceso ilícito a sistemas informáticos, conocido como *"cracking",* siendo preciso señalar que la actividad de *"hackeo"* también ya se encuentra prevista dentro del mismo precepto legal.

Nuestro artículo 282, en lo referente a las amenazas, contempla la conducta popularmente conocida como "*ciberbullying"* dentro de la descripción del tipo, se adecua perfectamente esta conducta.

Incluso, dentro de los nuevos preceptos legales creados en ese año, se aprecia una clara defensa contra el delito de lavado de dinero, pues dicho tipo penal de este numeral en comento, robustece el encuadramiento de dicha conducta con el precepto legal, contribuyendo a combatir la impunidad.

Todo lo anterior, de conformidad con la exposición de motivos de la Comisión de Justicia de nuestros Legisladores para modificar el Código Penal Federal.[52]

[52] http://gaceta.diputados.gob.mx/Gaceta/61/2012/mar/20120328-III.html#DictamenaD2
Gaceta Parlamentaria, año XV, número 3480-III, miércoles 28 de marzo del 2012.

Por el delito informático debe entenderse toda aquella conducta ilícita susceptible de ser sancionada por el Derecho Penal, consistente en el uso indebido de cualquier medio informático.

La OCDE lo define como cualquier conducta no ética ni autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.[53]

Ahora bien, cabe precisar que los delitos informáticos pueden dividirse en dos grupos:

- Los que utilizan la computadora como medio para realizar el delito.
- Los que utilizan la computadora como fin para realizar el delito.

Ahora, resulta menester enlistar los delitos informáticos reconocidos por la Organización de las Naciones Unidas como tales:

- Fraudes cometidos mediante manipulación de computadoras:
  a) Manipulación de los datos de entrada.
  b) Manipulación de programas.
  c) Manipulación de datos de salida.
  d) Fraude efectuado por manipulación informática.

- Falsificaciones informáticas
  a) Utilizando sistemas informáticos como objetos.
  b) Utilizando sistemas informáticos como instrumentos.

- Daños o modificaciones de programas o datos computarizados.

[53] 4 López Betancourt, Eduardo, Delitos en particular, México, Porrúa, 2004, p. 270

a) Sabotaje informático.

b) Virus.

c) Gusanos.

d) Bomba lógica o cronológica.

e) Acceso no autorizado a sistemas o servicios.

f) Piratas informáticos o hackers.

g) Reproducción no autorizada de programas informáticos con protección legal.

En este orden de ideas, precisamos que la forma de clasificar a los delitos informáticos, podría ser también:

- Delitos patrimoniales.
- Delitos de pornografía.
- Delincuencia Organizada.

Siendo así, que el primer supuesto se refiere a las practicas conocidas como *"Phishing"* consistiendo en envían correos electrónicos falsos a los usuarios de los bancos para hacerles creer que son por parte de la Institución de Crédito, recaban información personal sobre las tarjetas bancarias y causan prejuicios patrimoniales a los mismos.

Para evitar lo anterior, se recomiendo como mínimo:

- Tener una herramienta antivirus vigente y actualizado.
- Poseer herramientas anti intrusos.
- Tener un firewall personal.
- Tener autorizados parches de seguridad.
- Controlar las entradas y salidas de las unidades usb y disquetes para evitar las descargas de impresiones fotográficas, entre otras.

En cuanto al segundo tópico, se encuentra perfectamente detallado en el numeral 201 BIS del Código Penal Federal el delito de Pornografía mismo que dice al que

procure o facilite por cualquier medio el que uno o más menores de dieciocho años, con o sin su consentimiento, lo o los obligue o induzca a realizar actos de exhibicionismo corporal, lascivos o sexuales, con el objeto y fin de videograbarlos, fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, se le impondrán de cinco a diez años de prisión y de mil a dos mil días multa.

Resulta obvio que el legislador le importó muchísimo ser bastante claro, por lo que además agrego las conductas de fijar, grabar e imprimir datos de exhibicionismo corporal, también al que dirija y organice grupos de personas con esa actividad.[54]

El fenómeno de la pornografía en Internet, para Reyna Alfaro, se engloba dentro de los denominados delitos computacionales, al suponer una nueva manifestación del delito ofensas al pudor, cuya comisión afecta el bien jurídico de la libertad sexual.[55]

Ahora bien, respecto al tercer supuesto, el legislador estableció el requisito de que en todo momento el Procurador General de la República debe solicitar al Juez de Distrito permiso, fundado y motivado, para intervenir comunicaciones cuando tenga sospechas de que la persona que se investiga tiene relación con la delincuencia organizada.

Establece que más se puede intervenir, siendo el caso de comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores.

---

[54] Cassouz Ruiz, Jorge Esteban. Delitos Informáticos. Revista de la Judicatura Federal. Número 28. Página 231.

[55] Reyna Alfaro, Luis, "Pornografía e Internet: aspectos penales", AR: Revista de Derecho Informático, núm. 050, septiembre de 2002, http://www.alfa -redi.org/rdi-artículo.shtml?x=1449.

5.2 ACCIONES DE PREVENCIÓN EN CONTRA DEL DELITO INFORMÁTICO.

Al respecto no es ocioso señalar que en materia prevención, existe la Unidad de Ciberdelincuencia Preventiva, adscrita a la Secretaría de Seguridad Pública de la Ciudad de México, quienes son los encargados de monitorear constantemente la actividad en internet, incluso, elaborando *"Alertas"*[56] en las cuales advierten a la ciudadanía de no ser víctimas de los delitos informáticos, explicando la forma de actuar de los sujetos activos.[57]

En este sentido, resulta claro que la actividad que realiza la Secretaría resulta insuficiente, pues como lo mencioné en números anteriores del presente trabajo, no se realiza una investigación detallada sobre la Internet Obscura, por mencionar solo un ejemplo, además de que cabe el análisis, ¿Qué tanto es fructífero que esta investigación la realice la Secretaría de Seguridad Pública en vez de la Procuraduría General de Justicia, ya sea local o federal? Basta con recordar las funciones de cada dependencia, en opinión personal, debería ser encabezada por la Procuraduría, sin lugar a dudas.

Uno de los esfuerzos que la Secretaría de Educación Pública hace para prevenir los delitos informáticos son pláticas informativas dirigidas hacia los estudiantes de educación básica y media superior, acerca del uso responsable de las redes sociales y del Internet en general.[58]

Basta señalar, por ejemplo, que diversas dependencias de gobierno constantemente alertan a la ciudadanía para que tenga una mayor cultura y conocimiento acerca de los delitos informáticos, por ejemplo, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros de manera periódica alerta para evitar proporcionar datos personales a supuestos correos

---

56 http://data.ssp.cdmx.gob.mx/documentos/ciberdelincuencia/ciberalertas/Alerta%20Preventiva%20Ciberdelincuencia_No.19.pdf

57 http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html

58 http://www.sepyc.gob.mx/documentacion/Prevencion_del_Delito_Cibernetico.pdf

provenientes de Instituciones de crédito, correos que desde luego son falsos y solo funcionan para que previo a la recolección de datos personales, hagan mal uso de los mismos [59] esta práctica es conocida como *"Phising",* ya descrita anteriormente en el cuerpo del presente trabajo.

[59] http://www.forbes.com.mx/condusef-alerta-sobre-correo-falso-de-banamex-2/#gs.U9XMNCc

5.3 LEGISLACIÓN PENAL AL RESPECTO.

Para abordar este tópico, realizaré un análisis acerca de la legislación penal tanto local como federal acerca de los delitos informáticos.

El Código Penal Federal establece en el numeral 167, fracción VI lo siguiente:

Artículo 167.- Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:

> *"VI.- Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos;"*

De la lectura del anterior artículo, resulta claro la intención del legislador por encasillar la conducta descrita de naturaleza dolosa para la obtención de un fin lucrativo, puesto es que sin aquel elemento subjetivo de la conducta ni con la finalidad, cualquier intervención o interferencia no se consideraría delito.

Al respecto, los numerales 211 bis al 211 bis 7, rezan:

> *"Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa."*
>
> *"Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de*

uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes."

"Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente

en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública."

"Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa."

"Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero."

"Artículo 211 bis 6.- Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código."

"Artículo 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno."

Es preciso señalar que el día 17 de marzo del año 2000 se pretendió hacer una primera descripción de la conducta conocida como *"hacker"* y *"cracker"* atendiendo que se sancionaría aquellas actividades que alteren el sistema financiero, no siendo limitativo a este último, pues puede ser a cualquier medio informático.

Ahora bien, se puede señalar que también se intentó por parte del legislador, contemplar la conducta de piratería, sin embargo, no se especificó que se entendería como piratería cuando el medio comisivo sea el Internet o sea por medio de un delito informático.

Por lo que la reforma surgida de forma posterior, la de fecha 28 de marzo del 2012, viene a complementar el primer esfuerzo aquí descrito por parte del legislador, ya que se hace un detalle más preciso acerca de las conductas habituales conocidas por los "hacker" "cracker" y el "pishing" sin embargo, de esta última reforma, en el numeral 205 bis, en la fracción k, no fue contemplada para su adición al momento de publicar la reforma a nuestro Código Penal Federal.

Siendo que la hipotética fracción k que se propuso y al final, sin explicación alguna, no fue prevista para el proyecto final, debió quedar como sigue:

Artículo 205 Bis. Las sanciones señaladas en los artículos 200, 201, 202, 203 y 204 se aumentarán al doble de la que corresponda cuando el autor tuviere para con la víctima, alguna de las siguientes relaciones:

k) Quien se valga del uso o empleo de medios informáticos para generar relación de confianza o amistad con la víctima.

Resulta claro que la omisión de esta fracción, permite una brecha por la cual no se describe perfectamente este supuesto de delito informático.

Ahora bien, nuestro Código Penal para el Distrito Federal, señala en su apartado 231 fracción XIV:

"Artículo 231. Se impondrán las penas previstas en el artículo anterior, a quien:

xiv. Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores, independientemente de que los recursos no salgan de la institucion"

Cabe el análisis si realmente estamos ante los elementos que integran el delito de Fraude, en virtud de que esta fracción en comento, no contempla que por parte del sujeto activo se lleve al engaño o se aproveche de dicho engaño al sujeto pasivo, luego entonces, resulta obvio precisar que para la persona que realiza la conducta delictiva prevista desde el punto de vista de delito informático no requiere ni siquiera que el sujeto pasivo tenga conocimiento del perjuicio en su contra, que casi todas las veces se traduce en un perjuicio patrimonial, pues solo basta con que el activo tenga el conocimiento técnico suficiente para realizar dicha conducta reprochable por la Ley Penal.

También existen disposiciones que no son exclusivas del área penal, motivo del presente trabajo, como lo es la Ley Federal de Derechos de Autor, reglamentaria

del artículo 28 constitucional, así como la Ley de de Protección de Datos Personales en Posesión de Particulares, por mencionar algunas, que no son objeto del presento trabajo.

Ahora bien, a nivel Internacional, contamos con el listado de Delitos Informáticos que la Organización de las Naciones Unidas hizo al respecto, mismo que se encuentra al principio del presente documento y que robustecen lo contemplado por nuestros cuerpos normativos, tanto federal como local.

Respecto a lo dispuesto por la Organización de las Naciones Unidas, acerca de los delitos informáticos, destaca que si bien es cierto, el avance la sociedad por medio de la tecnología se da a una velocidad más vertiginosa, también lo es que dicha sociedad debe avanzar al mismo nivel respecto a la forma para prevenir y sancionar delitos de esta índole.

El documento en comento mencionado destaca que la escasa cuantificación de los delitos informáticos en el mundo, no permiten que los Estados tengan una adecuada planeación e implementación de políticas públicas pues no se cuenta con un parámetro real para realizar dicha aplicación.

CAPÍTULO VI.

DISPOSICIONES INTERNACIONALES

6.1 CONGRESO DE LAS NACIONES UNIDAS.

La ONU, por medio del 12 Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, llevado a cabo en Salvador, Brasil, del 12 al 19 de abril del año 2010 ha descrito que uno de los problemas por lo cual la cuantificación falla, es en virtud de no ser posible la estimación financiera respecto al daño patrimonial que los delitos informáticos ocasionan.

De acuerdo a algunas fuentes, solo en Estados Unidos, las pérdidas que se obtiene por la comisión de los delitos informáticos, asciende a cerca de los sesenta y siete mil millones de dólares. [60]

Por lo que resulta obvio que si existe un detalle exacto acerca de la cuantificación de los delitos informáticos, también lo es que exista una falta de documentación acerca del número de víctimas y un reconocimiento estricto de las conductas que son reconocidas como delitos informáticos, a modo de engrosar las ya descritas y contemplar o considerar las nuevas descubiertas.

Ahora bien, en esta tesitura existe una preocupación real acerca de la dimensión trasnacional de este fenómeno delictivo tan poco conocido.

En virtud de que el Internet se concibió primeramente como un proyecto militar, tema ya expuesto anteriormente en este mismo trabajo, y que a raíz de la comercialización de Internet, el fenómeno se vuelve desde luego de manera casi instantánea en una situación internacional.

Además de lo anterior, los delitos informáticos adquieren una zona de internacionalización en virtud de que prácticamente en todo el mundo, cualquier persona puede por medio del correo electrónico, enviar un correo a otra que se encuentre conectada a Internet a otra parte del mundo, por lo que si ese correo electrónico contaba con información maliciosa que la hacía portadora de algún virus o sistema necesario para ingresar a alguna base de datos sin autorización,

[60] Estados Unidos, Oficina Federal de Investigación, 2005 FBI Computer Crime Survey, pág. 10

resulta claro que el delito informático en cuestión tiene resonancia no solo en el país donde se envió el correo electrónico, sino también, en el país que evidentemente recibió dicha documentación maliciosa.

Lo anteriormente detallado contiene una problemática que obstaculiza la persecución de estos delitos, toda vez que, por ejemplo, en el año 2000 en Filipinas fue creado y desarrollado un virus informático denominado *"LOVEBUG"* mismo que infecto a millones de computadoras en todo el mundo, extrayendo información sensible, tanto de servidores privados como de instancias gubernamentales a nivel internacional.[61] Esta situación, hizo que la investigación pertinente del delito se viera entorpecida toda vez que en aquel país, Filipinas, no estaba ni siquiera contemplada como un actuar ilícito, por lo tanto, no era reconocida como delito en su cuerpo normativo.

Por lo que resulta de suma importancia que converjan las legislaciones tanto locales como internacionales, entre iguales como frente a la otra, en el tema de delitos informáticos, por lo que se ha vuelto un tema prioritario para los países lograr erradicar con sitios seguros para los delincuentes realizar dicha actividad, toda vez que en esos sitios, estas conductas no son consideradas delito o peor aún, no son ni siquiera reconocidas estas conductas como algo tangible en su realidad.

Otra de las problemáticas que se da en algunas partes del mundo, es el hecho, de que si bien es cierto, se reconocen conductas iguales como delitos en diferentes países, el problema recae en que dichas conductas, tienen penalidades muy diferentes en esos países o consideran situaciones o requisitos diversos que

---

[61] Estados Unidos, Oficina General de Contabilidad, Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, testimonio prestado ante el Subcomité de Instituciones Financieras, Comité de Asuntos Bancarios, Urbanos y de la Vivienda, Senado de los Estados Unidos, informe de la Oficina General de Contabilidad GAO/T-AIMD-00-181 (Washington, D.C., mayo de 2000).

podrían hacer que en un país sea delito y en el otro ya no, por existir un supuesto que la normativa local contempla.[62]

Por lo que por ejemplo, en algunas partes del mundo puede ser delito subir a la red cierto contenido, y en otra parte del planeta, subir la misma información no es considerada delito, por lo que resulta obvio que el segundo supuesto representa una oportunidad para el delincuente poder ejercer su actividad sin ningún problema.

Por lo que resulta menester conocer que existen diversas formas para hacer frente al impacto trasnacional del delito informático y a la diferencia de las normas jurídicas penales.

[62] Los diferentes enfoques jurídicos que regulan el contenido son uno de los motivos por los que ciertos aspectos del contenido ilegal no están incluidos en el Convenio sobre la Ciberdelincuencia sino que se tratan en un protocolo adicional. Véase también El ciberdelito: Guía, cap. 2.5 (véase la nota de pie de página 2)

6.2 COMPATIBILIDAD DE LA LEGISLACIÓN.

Desde luego que la forma más eficaz para combatir al impacto trasnacional del delito informático es mediante el mejoramiento de la cooperación internacional desarrollando legislación pertinente.

En el año 2002, el *"Commonwealth"* que se entiende para referirnos a una comunidad política de diversos países, elaboró una Ley para referirnos al delito informático, misma Ley que contiene disposiciones sustantivas y procesales al respecto.

Resultando que la principal problemática es que dicha Ley solo aplicaba para los países miembros de la comunidad política mencionada anteriormente, por lo que los países que no eran miembros, podían seguir teniendo actividad delincuencial con impacto y consecuencias en el resto del mundo.

Ahora bien, la Unión Europea ha realizado diversos esfuerzos por armonizar las disposiciones aplicables respecto al delito informático, aunque solo aplica para los veintisiete países miembros.

Resulta vital precisar que a diferencia de lo que ocurre en las demás comunidades políticas, los acuerdos logrados por parte de la Unión Europea tienen carácter vinculante entre todos los países que integran dicha Unión.

Algunos de dichos acuerdos alcanzados por la Unión Europea, de forma enunciativa únicamente, son:[63]

- Decisión marco 2000/413/JHA del Consejo de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo

[63] 12 Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Salvador (Brasil) del 12 al 19 de abril del 2010. Página 7.

- decisión marco 2004/68/JHA del Consejo de la Unión Europea sobre la lucha contra la explotación sexual de los niños y la pornografía infantil
- la decisión marco 2005/222/JHA del Consejo de la Unión Europea sobre los ataques contra los sistemas de información

Ahora bien, dicha Comunidad Europea, ha realizado diversos instrumentos internacionales para el combate a los delitos informáticos, siendo que el instrumento más conocido es el Convenio sobre Ciberdelincuencia, llevado a cabo entre 1997 y 2001, mismo que contiene disposiciones sustantivas, adjetivas y de cooperación internacional.

Destaca que para el año 2009, ya había sido firmado por cuarenta y seis países y ratificado por veintiséis países miembros.

6.3 TERRITORIALIZACIÓN.

Una de las principales dificultades con las que los múltiples esfuerzos internacionales para hacer frente a los delitos informáticos son las legislaciones locales, pus si bien es cierto, existe en la mayoría de las veces una gran voluntad política para realizar dichos acuerdos de cooperación por parte de los Estados miembros, también lo es que los cambios en las legislaciones locales respecto al tema a tratar son muy lentos, por lo que cuando por parte de algún país se logra la voluntad interna de realizar alguna modificación o propuesta al respecto, este esfuerzo siendo casi etéreo, pues los cambios tecnológicos siempre terminan por rebasar a la sociedad en comento y sus intentos de adecuación de los cuerpos normativos locales, por lo que no se consigue el objetivo principal, lograr la territorialización del internet.

Resulta obvio que Internet está fuera de las fronteras físicas, por lo que su alcance es internacional e infinito, por lo que los Estados se han percatado de la importancia de voltear a ver a los proveedores de internet, exigiendo bloqueo a contenido delincuencial, como por ejemplo, pornografía infantil, en los paquetes de internet que proporcionan.

El principal tema a discusión al tratar este tópico, es sobre si al exigir el bloqueo a los proveedores de internet a ciertas páginas con contenido delincuencial al usuario cuando este intente ingresar, no se está excediendo los límites del Estado, cayendo en abusos y violaciones a Derechos Humanos, como por ejemplo, el acceso a internet.[64]

[64] Para obtener más información sobre el bloqueo de Internet y el equilibrio entre las libertades fundamentales, véase Cormac Callanan y otros, Internet Blocking: Balancing Cybercrime Responses in Democratic Societies (Dublín, Aconite Internet Solutions, octubre de 2009), caps. 6 y 7

6.4 DELINCUENCIA ORGANIZADA E INTERNET.

Al respecto cabe señalar que los delitos informáticos, si bien es cierto, pueden ser cometidos por una persona física en solitario, también es cierto, que pueden ser cometidos por un grupo de personas, que en su actuar, podrían conformar algún grupo de delincuencia organizada.

Conocer esto, resulta relevante ya que se puede aplicar de los instrumentos mencionados anteriormente acerca del combate a los delitos informáticos, los instrumentos acerca de Delincuencia Organizada, como por ejemplo, Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Al hablar de delincuencia organizada e internet, se tiene que distinguir entre los grupos de delincuencia organizada tradicionales que hacen uso del internet y la comisión de delitos informáticos por parte de grupos de delincuencia organizada.

Es decir, en el primer supuesto, al ser grupos de delincuencia organizada que no cuentan con antecedentes de la comisión de hechos delictuosos de carácter informático por medio de internet, únicamente utilizan internet en su modalidad de tecnologías de la información para la planeación de sus actividades diversas.

Sin embargo, el segundo supuesto, se refiere a grupos de delincuencia organizada, que estos sí utilizan el internet para su objetivo principal que es la comisión de diversos delitos de carácter informático.

Por lo que, el autor del presente trabajo, considera que las dos principales características de los grupos especializados de delincuencia organizada en delitos informáticos son:

- Los grupos dedicados al delito cibernético suelen tener una estructura más flexible y abierta, que permite la incorporación de nuevos miembros por un período de tiempo limitado.

- En muchos casos, los miembros de los grupos comunican entre sí exclusivamente en forma electrónica, sin tener nunca encuentros personales.

6.5 CONVENIO SOBRE LA CIBERDELINCUENCIA.

Al respecto, cabe señalar que los países miembros que suscribieron y ratificaron dicho instrumento son los países miembros del Consejo de Europa, bajo la consigna de que el objetivo principal era lograr una unión más estrecha ente los países miembros.

El instrumento jurídico en comento se elabora por la necesidad de contar con una política penal en común para hacer frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada, y la mejora de la cooperación internacional.[65]

Cabe destacar que dicho Instrumento es realizado en el contexto de identificar que es del conocimiento para los países miembros, que la digitalización que la globalización impuso, trajo aparejado una cambio tanto de la sociedad como de la forma en que esta se relaciona, positiva o negativamente, por lo que hablando del segundo supuesto, existen nuevas y más variadas formas de delinquir, siendo obligación inmediata del Estado, entendiéndose los Estados miembros, contar con Instituciones más eficaces y a la vanguardia para hacer frente a estas conductas.

Por lo que es necesario que este instrumento internacional sea de efectiva aplicación, toda vez que es de vital importancia, combatir a los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sitios que integran las redes de la información, así como los delitos que integran el uso ilícito de dichas redes, datos e intercambio multimedia de información maliciosa.

El convenio en comento, se desarrolló, tomando en cuenta desde luego la Convención sobre los Derechos del Niño de las Naciones Unidas, suscrito en 1989

[65] Convenio sobre la Ciberdelincuencia. Budapest, Hungría. 23 de noviembre del 2001. Preámbulo.

y el Convenio sobre la peor forma de trabajo infantil de la Organización Internacional del Trabajo, suscrito en el año de 1999.[66]

Por lo que los países miembros elaboran el documento en cuestión, mismo que contiene los siguientes preceptos que me atrevo a transcribir por ser de interés personal para su comentario:

CAPÍTULO I TERMINOLOGÍA.

Artículo 1 Definiciones.

A los efectos del presente Convenio:

A) Por sistema informático se entenderá todo tipo de dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí , siempre que uno de ellos o varios, permita el tratamiento automatizado de datos en ejecución de un programa.

B) 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.

C) Por proveedor de servicios se entenderá:

I.- Toda entidad pública o privada a los usuarios de sus servicios la posibilidad de comunicar por medio de sus servicios informáticos.

II.- Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.

D) Por datos sobre el tráfico se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y dirección de la comunicación o el tipo de servicio subyacente.

[66] Ibídem. Preámbulo.

Es de especial interés personal el comentario al respecto sobre este numeral, pues existe el concepto a nivel internacional de cada uno de los elementos que pudiesen intervenir en la comisión de delitos informáticos, a la vez de que se tiene perfectamente detallado que se entiende por los posibles entes que serían responsables por no proporcionar el servicio de cuerdo a los estándares internacionales para prevenir y combatir los delitos informáticos.

Ahora bien, a continuación, puntualizo las partes del Convenio, que enlistan las medidas que deberían adoptarse a nivel nacional:

> ***CAPÍTULO II MEDIDAS QUE DEBERÁN ADOPATARSE A NIVEL NACIONAL.***
>
> ***Sección 1- Derecho Penal Sustantivo.***
>
> *Título 1- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.*
>
> *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 ilegitimo 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.*

Al respecto del numeral anteriormente transcrito, cabe puntualizar, que si bien es cierto, en nuestro Código Penal Federal se encuentra descrita la conducta delictiva del acceso ilícito a las bases de datos para recolectar información no consentida, también lo es, que es que a mí parecer el numeral citado del instrumento

internacional está incompleto, pues debería contemplar los supuestos que el ordenamiento jurídico sustantivo federal dispone, mismo que son todos y cada uno:

Artículo 211 bis 1 al 7 del código penal federal relativo al acceso ilícito a sistemas y equipos de informática

Bis 1: al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas protegidos por algún mecanismo de seguridad se le impondrán de 6 meses a 2 años de prisión y de 100 a 300 días de multa

Bis 2: al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática del estado, prot egidos por algún mecanismo de seguridad se le impondrán de uno a cuatro años de prisión y de 200 a 600 días de multa

Bis 3: al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información que contengan, se le impondrán de 2 a 8 años de prisión y de 300 a 900 dias de multa

Bis 4: al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de seguridad, se le impondrán de 6 meses a 4 años de prisión y de 100 a 300 dias de multa

Bis 5: al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de 3 meses a 2 años de prisión y de 100 a 300 dias de multa

Bis 6: para los efectos de los artículos bis 4 y bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este código.

Bis 7: las penas previstas es este capítulo se aumentaran hasta en una mitad cuando la información obtenida se utilice en provecho o ajeno.

Es de apreciarse, que nuestro ordenamiento contempla mayores supuestos a lo dispuesto en el instrumento internacional.

Ahora bien, el Convenio Internacional en su numeral 3, contempla detalladamente como se da la interceptación ilícita, mismo que reza:

> ***Artículo 3 - Interceptación ilícita***
>
> *Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.*

En lo descrito anteriormente, se aprecia que nuestro ordenamiento legal aplicable, no se aprecia todos y cada uno de los supuestos detallados para que se encuadre la interceptación ilícita, por lo que de aquí, nuestros legisladores podrían engrosar o enriquecer nuestro tipo penal para no dejar en indefensión al ciudadano.

Al respecto al numeral siete del Convenio sobre delincuencia contempla:

> ***Título 2 - Delitos informáticos***
>
> ***Artículo 7 - Falsificación informática***
>
> *Cada Parte adoptar· 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.*

Cabe especial pronunciamiento al respecto por la última parte, al dar la posibilidad de que exista una intención fraudulenta o una intención delictiva, lo cual, hablando acerca de nuestro sistema penal, significa que no se pude cometer los delitos informáticos de manera culposa, pues es una requisito indispensable el elemento subjetivo de dolo para su comisión, en virtud de que nos encontraríamos con una persona con los conocimientos técnicos-informáticos necesarios y suficientes para su llevar a cabo su actividad delictiva, lo que no sería creíble presupuestar que dicha conducta el sujeto activo la materializó sin la intención de cometerla o no previendo su consecuencia material.

Ahora bien, existe un supuesto en el Convenio Internacional hay un apartado que llamó poderosamente mi atención, el cual reza:

> ***Artículo 9 - Delitos relacionados con la pornografía infantil:***
>
> *A los efectos del anterior apartado 1, por pornografía infantil se entenderá todo material pornográfico que contenga la representación visual de:*
>
> *b) una persona que parezca un menor comportándose de una forma sexualmente explícita;*

Cabe la pregunta natura, ¿Qué pasaría si después se descubre que esa persona, el sujeto pasivo, no es menor de edad? Estaríamos ante un supuesto no previsto por el Instrumento Internacional, toda vez que si bien en cierto se pensaba que se encontraría la situación ante un delito de pornografía infantil, que también existe en nuestro ordenamiento federal y local, en todos y cada uno de los supuestos que dichos tipos penales contemplan y requieren, pero a la vez, al saberse que el sujeto pasivo, simplemente por el conjunto de sus características físicas parecía un menor de edad, de acuerdo a lo contemplado por la legislación local e internacional, sin embargo, resulta que es mayor de edad y sin ninguna causa de interdicción que pudiera mediar por él, entonces estaríamos, tal vez, solo como

posibilidad, ante otra figura delictiva, pero el caso concreto, quedaría ante un escenario no previsto.

También resulta necesario el comentario al respecto del siguiente artículo del Convenio Internacional:

> ***Título 5 - Otras formas de responsabilidad y de sanciones***
>
> ***Artículo 11 - Tentativa y complicidad***
>
> *1- Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.*

Al respecto, resulta obvio, que nuestro ordenamiento legal, tanto el federal como el local, no contemplan la puesta en peligro del bien jurídico tutelado, como para tipificar la comisión del delito informático en grado de tentativa, lo cual, además de no estar en concordancia con los estándares internacionales, suprime una parte del supuesto contemplado en aquel, que permitiría un porcentaje de impunidad específicamente en dicho supuesto.

Ahora bien, los siguientes numerales, de ser contemplados en nuestros ordenamientos jurídicos sustantivos federales y locales, permitirían presupuestar todos y cada uno de los escenarios y supuestos que requieren los delitos informáticos para su comisión, por ejemplo:

> **Título 3 - Orden de presentación**
>
> **Artículo 18 - Orden de presentación**
>
> *Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:*
>
> *a) a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y*

b) a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

Artículo 20 - Obtención en tiempo real de datos sobre el tráfico.

Cada Parte adoptar· las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:

a) obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b) obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

1.- a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

2.- a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar.

Los anteriores numerales, permiten apreciar algunos de los supuestos técnicos que nuestros legisladores no consideraron en las posteriores reformas hechas a nuestros Códigos Penales, en especial el Federal, al intentar tipificar el delito informático.

Estos numerales, desde luego que solo son enunciativos más no limitativos del Convenio Internacional en su totalidad, permiten referirnos que de conformidad a un adecuado control de convencionalidad y a un control difuso de la constitución, todos los Órganos Jurisdiccionales tienen la obligación, de oficio o a petición de parte, de aplicarlos.

En virtud de que el Estado Mexicano no forma parte de los Estados que conformaron la suscripción y ratificación al Instrumento en comento, así como tampoco formó parte de su elaboración, podría solicitar su adhesión, por medio de

algún Estado que si haya estado en algún supuesto anteriormente mencionado, desde luego, implicando la aceptación de su jurisdicción, o en su defecto, iniciar el cabildeo necesario para que logre formar un Instrumento Internacional con el Comité del cual si sea parte, en aras de lograr un Estado de Derecho.

CONCLUSIONES.

Resulta relevante precisar que una de las características del Estado de Derecho es garantizar que no exista la impunidad entre los gobernados, con mayor relevancia respecto a criterios internacionales acerca de los Derechos Humanos y el Acceso a la Justicia.

En esta tesitura, siendo que nos encontramos en una era digital, donde la globalización ha impuesto formas de vida y con ello, resulta claro, también ha propuesto formas de impartir justicia, cabe como ejemplo ,las llamadas cortes cibernéticas que funcionan en Estados Unidos dese hace una década.

Por lo que en aras de la era digital y la adaptación a una sociedad de la información, resulta claro que el Estado debe tener perfectamente garantizado el acceso a la justicia, así como la sanción equitativa, justa y proporcional para las conductas agrupadas como delitos informáticos.

Son esfuerzos acertados las reformas recientes en materia de delitos informáticos hechas a nuestro cuerpo normativo federal en materia penal, sin embargo, debe ir acompañas de una difusión, creando conciencia, de una adecuada cultura jurídica que permita, primeramente reconocer que es un delito informático, y después saber que existen formas de castigarlo, pero principalmente formas de prevenirlo.

Por lo que resultando obvio que si bien es cierto el Derecho evoluciona junto con la sociedad, es de naturaleza flexible, también lo es que la sociedad rebasó por mucho al Derecho, luego entonces, nosotros como operadores jurídicos debemos estar a la vanguardia de este tipos de temas que conllevan una sinergia entre Derecho e Informática.

Al respecto, es un gran aporte las definiciones del Derecho en este rubro, primeramente creando la llamada Jurismática, haciendo los juristas el esfuerzo por abarcar dentro del campo del Derecho, lo relacionado al área de la Informática.

Concepto que tiene su nacimiento en la década de los cincuenta, en el marco de la conocida *"Guerra Fría"* en los Estados Unidos, por lo que los avances significativos en este tópico se dan en dicho país y en Europa principalmente.

Posteriormente, el concepto de Jurismática se deja a un lado para dar cabida al nuevo y más amplio concepto de Derecho Informático, donde se reconocen no solamente los medios tecnológicos con los que todas las áreas de Derecho ven íntimamente relacionado su ejercicio diario, sino también, en hacer un esfuerzo por regular específicamente o complementar lo ya regulado que tiene su nacimiento en el Derecho pero su explotación total y cabal en la red.

En este orden de ideas, dentro del Derecho Informático, nos encontramos en el ramo penal con los delitos informáticos, que se diferencian del concepto conocido de delito, pues los primeros para ser tratados forzosamente requieren del uso tecnológico para su realización.

Por lo que la clasificación debe ser de acuerdo, hablando de delitos informáticos, según los bienes jurídicamente tutelados afectados.

Resulta menester que para tratar la regulación penal de los delitos informáticos, se requiere de un tratamiento multidisciplinario, pues para la materialización de dicho actos ilícitos se requiere de un alto grado de conocimiento técnico.

Por lo que en nuestro país, para combatir la alta tasa de impunidad que impera, es papel preponderante, que exista una cultura de la legalidad para que la ciudadanía que no cuenta con los conocimientos técnicos adecuados o con la suficiente pericia para ingresar a sistemas informáticos, por lo menos sepa que hacer para prevenir dichas conductas, primeramente reconociendo que existen y su existencia es un delito.

Por lo que es imperante que exista una política pública donde se concientice a la población de que la principal forma de contribuir, desde el ámbito de sus principales ocupaciones, es denunciar ante la Representación Social, cuando sean

víctimas de algún delito informático o sepan de alguien que es víctima del mismo y puedan orientarle de la importancia que tiene denunciar, pues sin ese requisito, todo lo demás es estéril, ya que es el primer supuesto, llamado requisito de procedibilidad.

Del estudio del presente trabajo, es de notar, que los esfuerzos nacionales pro regular este tópico, no contemplan tipos penales específicos, sino más bien, presupuestos o características circundantes.

Es decir, se requiere para la elaboración de estos tipos penales, forzosamente un equipo multidisciplinario, para que sin la necesidad de caer en palabras en inglés, se pueda dar concepto a situaciones que en nuestro vocabulario técnico de este tema solo es posible con los llamados *"anglicismos".*

Por lo que considero, sería de gran relevancia, que se creara un capítulo específico denominado "*delitos informáticos"* que contemple todas y cada una de las actividades y supuestos de estas conductas, así como todos y cada uno de los medios comisivos para su materialización, a la luz desde luego de la Teoría del Delito.

Ya que nuestros ordenamientos jurídicos sustantivos penales, tanto el federal como el local, únicamente contemplan supuestos, pero complementarios para otros tipos penales, más no se habla en concreto de delito informático como tal.

Por lo que del presente trabajo, se desprende que la aparición del Internet en nuestro país es reciente, así como la familiarización de la sociedad con la misma, además de que el acceso a la súper carretera de la información en México queda corto respecto a sus similares a nivel internacional.

En virtud de lo anterior, el tema de delitos informáticos no debe ser tratado como un complemento de tipos penales ya existentes, ni como un asunto meramente doctrinal, debe ser atendido como un delito independiente de los demás y con la importancia de que el Estado esté preparado para hacer frente a dichas

conductas, pues la globalización y la sociedad de la información es ya una realidad que pareciera rebasó a nuestras instituciones jurídicas, y es obligación de los operadores jurídicos estar conscientes de esto para estar en posibilidad de tratarlo de manera eficiente, desde el ámbito de competencia de cada uno, para contribuir al Estado de Derecho.

BIBLIOGRAFÍA.

- Bacigalupo, Enrique. Lineamientos de la teoría del delito. Juricentro, San José, 1985.

- Díaz-Aranda, Enrique. Lecciones de Derecho Penal para el Nuevo Sistema de Justicia en México. Instituto de Investigaciones Jurídicas 2015.

- Loevinger, L. "The Next Step Forward" en Minessota Law Review, Vol. XXXIV, 1949.

- Téllez Valdés, Julio. Derecho Informático. 3ª edición, Editorial McGraw Hill. Serie Jurídica. México. 2003.

- Castellanos Tena, Fernando. Lineamientos Elementales del Derecho Penal. Porrúa. México. 1986.

- Guazmayan Ruiz, Carlos. Internet y la Investigación Científica. El uso de los medios y las nuevas tecnologías en la educación. Alma Mater Magisterio. Primera Edición 2004.

- Heffer, Jean. Launay, Michael. La Guerra Fría 1945-1972. Ediciones Akal, S.A. 1992.

- Hernández Hernández, Selene Guadalupe. Análisis Jurídico sobre la necesidad de crear un capítulo especial denominado delitos cometidos a través de la utilización de medios informáticos dentro del Código Penal para el Distrito Federal. México. Aragón. 2008.

- Kant, Immanuel. La Metafísica.
- Koenigsberger, Gloria. Los Inicios del Internet en México. 2014
- López Betancourt, Eduardo, Delitos en particular, México, Porrúa, 2004.

- Losano, M. Giuscibernética. 1960.
- Machicado, J. Concepto del delito. La Paz, Bolivia. Apuntes Jurídicos. 2010.
- Mayer Ernest, Max. Derecho Penal Parte General. Editorial B de F. 2007.
- Muñoz Conde, Francisco y García Arán, Mercedes, Derecho Penal. Parte General, Tirant lo blanch Valencia, 2002, p. 203.
- Pellegrino, Rossi. Lineamientos Elementales de Derecho Penal. Porrúa. 2001.
- Rodríguez, Erika. Historia de Internet en México.
- Roxin, Claus, Derecho penal. Parte general. Fundamentos. La estructura de la teoría del delito, trad. de Diego Manuel Luzón Peña, Miguel Días y García Conlledo, y Javier de Vicente Remesal, 2ª ed., Civitas, Madrid. 1997.
- Terragni, Marco Antonio. Estudios sobre la parte general del Derecho Penal. Universidad Nacional del Litoral, Santa Fe, Argentina. 2000. Página 104.
- Welzel, Hans, Estudios de derecho penal. Estudios sobre el sistema de derecho penal. Causalidad y acción. Derecho penal y Filosofía, Editorial B de F. Montevideo-Buenos Aires. 2003
- Zaffaroni, Eugenio Raúl. Manual de derecho Penal. Parte General. 4ª reimpresión de la 2ª edición. Cárdenas, México D.F., 1998, Página 18.

REVISTAS:

- Cassouz Ruiz, Jorge Esteban. Delitos Informáticos. Revista de la Judicatura Federal. Número 28.
- Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Salvador (Brasil) del 12 al 19 de abril del 2010.
- De la realidad virtual a la realidad jurídica. Instituto de Investigaciones Jurídicas. Primera edición 1998. México
- Gayosso, Blanca. ¿Cómo se conectó México al Internet? Revista UNAM. ¿Crecimiento de uno o de todos?
- Instituto Nacional de Estadística y Geografía (México). Estadísticas sobre disponibilidad y uso de tecnología de la información y comunicación en los hogares. 2013. Página 42
- Ovilla Bueno, Rocío. Boletín Mexicano de Derecho Comparado número 92. Internet y Derecho.

ENLACES.

- http://gaceta.diputados.gob.mx/Gaceta/61/2012/mar/20120328-III.html#DictamenaD2
- http://www.revista.unam.mx/vol.4/num4/art7/ago_art7.pdf
- http://conceptodefinicion.de/internet/
- http://archivo.eluniversal.com.mx/articulos/55127.html
- http://www.conacytprensa.mx/index.php/ciencia/humanidades/7839-historia-de-internet-en-mexico-reportaje
- https://normatividadinfo6104.wordpress.com/2015/06/18/articulo-211-bis-1-al-7-del-codigo-penal-federal-relativo-al-acceso-ilicito-a-sistemas-y-equipos-de-informatica/
- http://derechomx.blogspot.mx/2008/08/teora -del-delito.html
- https://jorgemachicado.blogspot.mx/2009/03/causas -de-inculpabilidad.html
- http://www.diputados.gob.mx/LeyesBiblio/pdf/9_180716.pdf

LEGISLACIÓN.

- Constitución Política de los Estados Unidos Mexicanos.
- Congreso de las Naciones Unidad sobre Prevención del Delito y Justicia Penal.
- Código Penal Federal.
- Código Penal del Distrito Federal.
- Ley Federal del Derecho de Autor.