Delitos informáticos en México

Jorge Esteban Cassou Ruiz*

Y Jehová levantó jueces que los librasen
de mano de los que los despojaban

Jueces 2:16

SUMARIO: I. *Introducción*. II. *Internet*. III. *Jurisdicción y competencia*. IV. *Delitos informáticos*. V. *Conclusiones*. VI. *Glosario*. *Referencias*.

I. Introducción

En el año de 1975, fecha en que se creó la primera PC, difícilmente se podría vislumbrar la complejidad en el manejo de la información que se generaría a través de la red que se originó en 1963, pero que era de pocos conocidos, dado que su utilización se restringía al campo militar, tecnológico y universitario (ARPA); sin embargo, la masificación y disminución en los costos de las computadoras personales, así como la apertura de la red, que cambió su denominación a Internet, dio inicio a la formación de un mundo virtual, con ilimitadas posibilidades, lo que a la postre trajo consigo grandes beneficios a la humanidad como un bien común, tan sólo por citar alguno: la ventaja de la comunicación al instante entre dos países situados en los extremos del globo terráqueo, a la par de lo anterior, también se generaron serios problemas en relación con el uso y abuso de tal producto tecnológico, la incorporación del Internet al mundo real fue avasallador de tal manera que los sistemas

* Secretario adscrito al Juzgado Tercero de Distrito en el Estado de Veracruz.

jurídicos de las naciones no se encontraban preparadas con los mecanismos legales necesarios para afrontar dicha problemática. México, no fue la excepción, lo que dio lugar a que se generaran congresos internacionales para intentar regular en qué casos debían considerarse ilícitas determinadas conductas ejecutadas a través del uso del Internet, se gestaron nuevas denominaciones de delito, entre otras, delito informático, ciberdelito, etcétera, en nuestro país fue hasta el año de 1999 en que se incorporó a la legislación punitiva los delitos informáticos, aunque cabe destacar que diversos ordenamientos comprenden algunas figuras lesivas genéricas en las que bien se puede integrar conductas delictivas llevadas a cabo por el uso de Internet, el propósito de esta tesina es denotar los signos distintivos de los delitos informáticos y su análisis a través de la jurisdicción y competencia de nuestro país, a fin de visualizar la complejidad que representa en algunos casos la ubicación de los sujetos activos del delito, así como también la complejidad que resulta para el Estado la persecución de muchos ilícitos informáticos con motivo del derecho constitucional a la no intervención de comunicaciones privadas: el objeto de estudio es vasto y amerita no tan sólo una mirada de reflexión y análisis, sino un estudio reposado, metódico y digno de destacar en una serie de trabajos que, desde luego, no se logra acotar con estas breves líneas.

II. Internet

1. *La complejidad del Internet*

No existe el propósito aquí de hacer un análisis exhaustivo sobre lo que es la red Internet y su funcionamiento, pero sí debemos dar algunas pautas de qué es para poder continuar y esclarecer como surgen y se actualizan conductas como delitos, que se han denominado en no pocos países delitos informáticos.

La Internet es una red de computadoras conectadas entre sí. Esta red permite el intercambio de información. A fin de poder intercambiar información entre diferentes computadoras ubicadas en distintas partes del mundo se utiliza un lenguaje común a todas las máquinas. Este lenguaje se conoce como protocolo.[1]

[1] Barriuso Ruiz, Carlos, *La contratación electrónica*, Madrid, Dykison, S.L., 2002, p. 37.

A su vez, este intercambio de información crea un universo virtual, diferente del universo físico conocido. Este espacio universal o ciberespacio no tiene la localización fija, esto es, no se puede ubicar el lugar en donde se asienta.

Una de las características de este ciberespacio es que está formado por información contenida en medios electrónicos de almacenamiento y que estos medios de almacenamiento son de orden físico, por lo que en última instancia esa información esa ubicada en cierto lugar físico territorial, pero puede ser accedida desde cualquier parte del mundo.

Dentro del ciberespacio o del espacio virtual, es decir dentro de la red, existen diferentes métodos de comunicación, cada uno de ellos acorde con una finalidad. Así tenemos el mail que funciona como un correo tradicional, el FTP que funciona como el sistema de intercambio de libros de la biblioteca. Existe uno de estos servicios que ha cobrado más fuerza que los demás y es el servicio WEB, consiste en una "página" en la que se coloca cierto tipo de información sobre algún tema en particular. El servicio funciona como un tabloide de anuncios o como un sistema de reparto de propaganda.[2]

El Internet como vehículo no tan sólo de la información, sino de medios para llevar a cabo actos de comercio como compras, rentas, arrendamientos, etcétera, ha propiciado una revolución en el mundo entero, de ahí que haya sido comparado al tercer movimiento de cambio de la humanidad, los dos primeros fueron el manejo de la agricultura y el segundo la revolución industrial; por ello se le ha considerado un prodigio para el desarrollo de un gran número de actividades del ser humano, visto de este modo se podría estimar que nada de malo tiene un bien accesible a la humanidad a través de corriente eléctrica y un equipo PC de bajo costo, aunque actualmente hay tantas innovaciones tecnológicas que el Internet corre incluso a través del teléfono celular; sin embargo, el Internet también representa un gran reto y problema, nos referimos a que ha sido utilizado cono vehículo para llevar a cabo conductas que han propiciado en el menor de los daños intromisión a la privacidad de las comunicaciones, y en otras situaciones han causado graves daños al patrimonio de las personas e incluso también ha dado pauta, a que individuos conformen bandas de delincuencia organizada que por su nivel de tecnificación han llevado a cabo conductas graves, este fenómeno

[2] Zabale, Ezequiel, "La competencia en materia de acciones civiles o penales derivadas del uso de la red Internet", *Derechos Informáticos*, Argentina, 2002, pp. 121-131.

que tomó por sorpresa a muchos gobiernos, y que a pesar de los intentos por lograr un consenso entre los diversos países a fin de tipificar los delitos informáticos ha sido lento en comparación con las actividades delictivas, lo que ha propiciado que a los esfuerzos de los diversos Estados, se sumen incluso acciones de instituciones particulares para tratar de agilizar y controlar mejor el flujo de la información, así como restringir en la medida de lo posible las conductas delictivas a través de mecanismos tecnológicos.

Un ejemplo de lo anterior son los esfuerzos de las empresas e instituciones privadas por "blindar" sus sistemas de acceso a la información y así evitar fugas o desvíos de numerario, las instituciones que a nuestro modo de ver han puesto especial énfasis en esa autoprotección y en defensa de sus clientes son las instituciones de crédito.

2. *¿Quién es quién en el Internet?*

La red se integra por diferentes actores (usuarios, proveedores de acceso, proveedores de *hosting* y de *housting*).

El usuario es la persona física o jurídica que mantiene la página, el titular y el encargado de la página.

El proveedor de acceso a Internet es la empresa que se dedica a conectar a los usuarios individuales a la red a cambio de un precio o canon, generalmente mensual.

Por último, el proveedor de alojamiento o *housing* es aquella empresa que destina parte de su sistema o de su espacio virtual para alojar la página de una persona.

El proveedor de acceso en la mayoría de los casos es local al lugar del usuario, pero quien brinda el housing y/o el hosting puede estar en cualquier lugar del mundo.

En el caso, el proveedor de alojamiento, es decir el lugar en donde se aloja la página, puede ser a modo de ejemplo el conocido portal yahoo.com cuyos servidores se encuentran en los EE.UU. y su página principal se indica como www.yahoo.com.[3]

Tales referentes que de manera breve y sencilla explicitan la funcionalidad de cada uno de los actores en la red, se complican en grado sumo cuando

[3] *Idem*.

debe aplicarse el derecho, concretamente por cuanto hace a lo que es la legislación penal.

Esto es, porque un usuario que acceda al servicio del Internet en los Estados Unidos de Norte América, puede estar llevando a cabo conductas delictivas que se ejecuten materialmente en un diverso país, esa situación dificulta, desde luego la aplicación del derecho penal, porque por principio y a fin de cumplir con el marco normativo básico, se debe establecer la existencia del delito, posteriormente tiene que identificarse al sujeto activo, aspecto que en tratándose de ilícitos que se llevan a cabo a través del Internet no se facilita, dado el incipiente impulso que se ha dado a la materia de informática forense,[4] aún ubicando la identidad del trasgresor de la ley penal es necesario su enjuiciamiento con las formalidades esenciales del procedimiento, lo que se torna más difícil si como ya se destacó la conducta lesiva se llevó a cabo en un diverso país, es por ello que la necesidad que impone la Constitución en nuestro país de seguir con un debido proceso legal, en el que se cumplan con las formalidades esenciales del procedimiento, se dificulta en relación con los delitos informáticos, desde luego, existen algunos avances en cuanto a la configuración de dichos delitos en la ley penal, así como a mecanismos para lograr con técnicas forenses en materia de informática la ubicación del lugar en que se llevó a cabo la conducta delictuosa; sin embargo, el problema se complica para lograr la identificación del sujeto activo en un delito que difícilmente deja huellas y rastros a seguir, en este sentido, se han distinguido dos figuras delictivas a las que se les ha denominado el *phishing* así como el *trapping*, las que conducen a la utilización, obtención, transferencia o disposición indebida de fondos de los clientes de las instituciones de crédito, como su resultado real y tangible, incluso puede darse el caso en que intervengan también funcionarios o empleados de las instituciones bancarias.[5]

[4] Batiz Álvarez, Verónica, "Panorama general del marco jurídico en materia informática en México", *AR: Revista de Derecho Informático*, núm. 066, enero de 2004, http://www.alfa-redi.org/rdi-artículo.shtml?x=1246.

[5] Campoli, Gabriel Andres, "Los dos delitos más comunes y controversiales por medios informáticos: clonación de tarjetas de crédito y phising o transferencias electrónicas y legítimas", *AR: Revista de Derecho Informático*, núm. 101, diciembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=8083.

Citibank México desarrolló una unidad de computo forense, cuyos objetivos se centran en dos aspectos, el primero, realizar un análisis del equipo de computo sobre lo que ya pasó, en la que generalmente se trabaja sobre el disco duro del usuario, en este caso del cliente del banco que ha denunciado la sustracción o merma de su capital al ser víctima de un ataque informático; y el segundo aspecto se enfoca a que en vivo se conecte a la computadora y se pueda analizar el programa o aplicación.[6]

Por cuanto este tópico se ha legislado en la materia del computo forense, en el que diversos ordenamientos se limitan a otorgarles valor probatorio a los documentos o instrumentos que se obtienen por medios electrónicos.

3. *Ética en el manejo del Internet*

Al producirse la interacción mundial a través del Internet, es necesario para algunos establecer reglas básicas de comportamiento por parte del usuario, así como de los prestadores del servicio; por el contrario, existe quienes piensan que al ser el Internet un bien de la humanidad debe seguir un patrón de comportamiento libre en el que el recorrido por lo que se ha denominado la supercarretera de la información no se limite, y sólo esté sujeta a la habilidad de cada usuario para conducirse en ese mundo virtual; a nuestro modo de ver estimamos que sí deben existir reglas de etiqueta del comportamiento por parte de los usuarios, dicho de otro modo, como lo afirma Raz, aun en una sociedad de ángeles es menester crear reglas para que sus intereses no choquen entre sí, luego entonces, ante un sistema de comunicación mundial, que comprende una gran disparidad de cultura, edad, educación, no tan sólo es congruente sino indispensable crear un manual del comportamiento del usuario, manual que no debe limitarse a un estadio nacional, sino a un plano internacional, con la distinción de que no debe encontrarse elevado a la categoría de una norma con todos sus atributos legales, pero que sí debe servir de patrón para una mejor interacción en el Internet, y para desmotivar en principio, conductas reprobables, así como conductas lesivas.

[6] Videoconferencia "Delitos cibernéticos", transmitida a distancia 17 abril 2008, Consejo de la Judicatura Federal, Instituto de la Judicatura Federal, Ext. Veracruz.

Uno de los aspectos a destacar y que más se queja el usuario, es la recepción del correo no deseado (spam), se parte de la base que el correo electrónico se diseñó para permitir una comunicación fluida, sencilla y a bajo costo, empero, esa ausencia de discriminación entre mensajes solicitados o no solicitados, dio lugar a ofertar productos en forma masiva, que generó el *spamming*, en nuestro país se pretende a partir de la protección al consumidor obligar al proveedor de servicios a respetar la decisión del consumidor de no recibir avisos comerciales.

En Estados Unidos, por ejemplo, se creó la ley federal de control del ataque de pornografía y marquetin no solicitado, en el que se logró el consenso de republicanos y demócratas, en un tema que se ha tornado irritante.[7]

La regulación del Internet es un enorme reto en razón de su carácter internacional y de la enorme cantidad de sitios que existen de tan variada índole e interés, a guisa de ejemplo las personas pueden jugar en casinos virtuales sin ninguna regulación, a la fecha actual se puede decir que el único contenido de Internet prohibido y sancionado en nuestro país es el de la pornografía infantil.

Lo anterior de manera somera da una idea de lo grave que resulta carecer de reglas de comportamiento en el Internet; por ello, consideramos que los valores fundamentales de la sociedad, con independencia de la raza, credo, cultura y educación, son necesarios para la interacción en ese mundo virtual, por lo que consideramos que al darse de alta una persona en el Internet debe ser conciente y actuar de buena fe, expresando los datos que corresponden a su identidad, de igual manera los prestadores de servicio deben exigir mayores requisitos para la autorización de direcciones electrónicas.

Cierto es, que solicitar lo anterior padece nimio y poco trascendente, pero debemos recordar que en un principio la relación contractual se generó bajo el principio de la buena fe, axioma que debe rescatarse para el vertiginoso mundo de las relaciones a través del Internet.

[7] Farinella, Flavio, "Algunas notas sobre el spamming y su regulación", *AR: Revista de Derecho Informático*, núm. 094, mayo de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=6102.

III. Jurisdicción y competencia

1. *Concepto*

Se acepta en forma genérica que la jurisdicción es la facultad que tiene el estado para administrar justicia en un caso concreto por medio de los órganos judiciales instituidos al efecto, para cumplir dicha finalidad se sostiene que la función reúne al menos los siguientes elementos, a saber: *notio:* facultad para compeler a las partes al proceso; *coertio:* facultad para emplear la fuerza pública para el cumplimiento de lo ordenado en el proceso; *judicium:* facultad de resolver el conflicto con carácter definitivo; y *executio:* facultad de ejecutar lo dispuesto, incluso mediante la fuerza pública de ser necesario.[8]

La competencia, en cambio, es la atribución legítima a un juez u otra autoridad para el conocimiento o resolución de un asunto.[9]

En el sistema judicial mexicano, existe la competencia múltiple, en la que corresponde a los tribunales de la federación, la competencia que corresponde a las entidades federativas, así como la que compete al Distrito Federal.

El artículo 104 de la Constitución Federal, establece que corresponde a los tribunales de la federación conocer de todas las controversias del orden criminal que se susciten sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales celebrados por el Estado mexicano.

En razón de ello existen tres órbitas de juzgados que operan sobre el mismo territorio pero que entienden en cuestiones materiales diferentes. Así, por ejemplo, en el Estado de Veracruz, existen tribunales federales, así como juzgados de dicha entidad federativa, ambos con poderes de actuación sobre el mismo ámbito territorial (en este caso el Estado de Veracruz) pero entienden sobre hechos materiales diferentes.

Mientras que los tribunales del estado de Veracruz, son competentes para conocer respecto de los delitos en los que se dilucidan conductas tipificadas por el Código Penal vigente en el estado, los tribunales federales conocen, por su parte, de las controversias del orden criminal que se suscitan sobre el cumplimiento y aplicación de leyes federales o de los tratados internacionales

[8] Palomar de Miguel, Juan, *Diccionario para juristas*, México, Porrúa, 2000, t. II, pp. 884-885.

[9] *Ídem*, t. I, pp. 335-336.

celebrados por el Estado mexicano. Además, los tribunales federales intervienen en los casos en que se solicite la extradición de una persona con motivo de la comisión de un delito.

La cuestión que trae el caso bajo análisis debe plantearse en los siguientes términos: Cuando se trata de una conducta lesiva cometida a través del Internet ¿debe comprenderse que la competencia corresponde a los tribunales de la federación o recae en la de las entidades federativas? y de obtenerse una respuesta en tal o cual sentido ¿existe algún motivo jurídico para establecer por qué debe ser uno u otro?

A nuestro modo de ver las respuestas se encontrarán justamente en el tipo de ordenamiento en que se legisle, esto es, no se encuentra restringido la penalización de los ilícitos que se cometen a través del Internet a un solo ámbito; sin embargo, a nuestro juicio y por razones que se expondrán a continuación consideramos más conveniente que los delitos que se generen a través del Internet sean del orden federal.

En efecto, como un primer argumento a favor de establecer que las conductas delictuosas ejecutadas a través de Internet se comprendan en la legislación federal, obedece a que con regular frecuencia se ejecutan por personas que físicamente se encuentran en un país extranjero, situación que desde luego dificulta en gran medida no tan sólo su identificación, sino también su enjuiciamiento.

Otro factor a tomar en cuenta es que el problema se reduce nuevamente a no entender quién o quiénes son los actores de la red y cuál es la funcionalidad de cada uno. Cierto, por lo general los órganos jurisdiccionales que atienden las consignaciones correspondientes desconocen y les resulta incomprensible el diferente rol que asume por un lado quien ha elaborado y sistematizado la página, que no es necesariamente la misma que presta el servicio de la página de Internet, e incluso, puede intervenir un tercero que sólo se encuentra al acecho para infiltrarse en la PC del usuario, todo ello genera que los procesos jurisdiccionales no se estructuren con una dirección adecuada e incluso con grandes limitantes para una entidad federativa, que conduce a que en muchas ocasiones queden impunes.

De ahí, que la transterritorialidad o trasnacionalidad, es un elemento clave para dilucidar la conveniencia de que los delitos informáticos sean de competencia de los tribunales de la federación; puesto que a quien le correspondería la investigación y persecución de los delitos sería al Ministerio

Público, de acuerdo con lo establece el artículo 21 Constitucional, órgano institucional que a través de la Procuraduría General de la República, es el que está dotado de mayores recursos financieros, así como mayor cobertura para seguir el estudio de los diferentes tipos de actividades ilícitas que se desarrollan a través de Internet, e incluso al unir esfuerzos con las diferentes corporaciones policiacas como lo puede ser la interpol, dado su carácter trasnacional, puede coadyuvar a la investigación de los hechos delictuosos, compartiendo información y estableciendo redes de comunicación a su vez, con otras instituciones de policías cibernéticas.[10]

En México ya existe una unidad especializada en delitos informáticos de la Procuraduría General de la República, por lo que sería más conveniente aprovechar los recursos y cobertura tecnológica que se le han asignado para tratar de contrarrestar los ilícitos informáticos que se cometen a través de Internet.

2. *Competencia en materia de acciones penales por el uso del Internet*

Las cuestiones de competencia han significado desde siempre una problemática de difícil resolución dentro del marco de cualquier sistema jurídico.

Los problemas de jurisdicción y competencia devienen desde hace mucho tiempo, tan sólo por citarlo, desde la generación del *ius commune*, el derecho como orden ha encontrado solución parcial ha dichos problemas a través de diferentes figuras, ya la declinatoria, ya las cuestiones de competencia, etcétera.

Sin embargo, como ya se destacó, la incorporación de nuevas tecnologías a la vida moderna ha traído consigo una nueva problemática jurídica. En consecuencia, surge una serie novedosa de planteamientos jurídicos y entre estos nuevos planteamientos se encuentra la naturaleza de los jueces que deben conocer de los antijurídicos cometidos a través de Internet.

La respuesta a nuestro modo de pensar es contundente, debe corresponder a los tribunales de la federación, por lo que lo ideal no es contemplar una

[10] Campoli, Gabriel Andrés, "Pasos hacia la reforma penal en materia de delitos informáticos en México", *AR: Revista de Derecho Informático*, núm. 079, febrero de 2005, http://www.alfa-redi.org/rdi-artículo.shtml?x=974.

serie de figuras jurídicas diseminadas a lo largo de diversos ordenamientos que conformen el sistema jurídico mexicano, sino que deben incluirse en una ley especial en la que de modo sistematizado aglutinen las diferentes conductas lesivas, esa clasificación y distinción no deberá ser determinante y terminal, porque el desarrollo y la innovación tecnológica, de modo irremediable conduce a que día a día, surjan nuevas y variadas conductas que generen afectación a terceros, por lo que es mejor no establecer conductas casuísticas en dicha ley especial.

También consideramos de especial relevancia, la formación del juez de instrucción que deba conocer de los delitos de dicha índole, su preparación debe ser acorde a las nuevas tecnologías que se aplican en materia de informática, sabido es que el juez es un conocedor de derecho, un experto en la materia, pero además de ello debe estar apoyado en un panel de expertos en informática que le provean de las aclaraciones a las dudas que surjan dentro de un proceso jurisdiccional, con independencia de los diferentes dictámenes periciales que las partes ofrezcan para clarificar los puntos en controversia; tal aportación consideramos sería de gran utilidad y beneficio para el mejor desarrollo y eficaz impartición de justicia.

3. *El derecho a la no intervención de las comunicaciones privadas*

En el *Diario Oficial de la Federación* del 3 de julio de 1996, se publicó el decreto mediante el cual se declararon reformados los artículos 16,20, fracción I y penúltimo párrafo, 22 y 73, fracción XXI, de la Constitución Política. Por lo que concierne al artículo 16, la reforma le adicionó dos párrafos, que pasan a ser el noveno y el décimo, por lo que también recorrió en orden progresivo los tres últimos párrafos.

La primera parte del párrafo noveno establece, como regla general, el carácter inviolable de cualquier tipo de comunicación privada, dentro de las cuales quedan incluidas las telefónicas y radiotelefónicas que se mencionan expresamente en la exposición de motivos. La inviolabilidad de las comunicaciones privadas forman parte del *derecho a la intimidad o a la privacía*, que ya se encontraba implícito en el primer párrafo del artículo 16 de la Constitución, en cuanto prevé la inviolabilidad del domicilio y de la correspondencia; y que ha sido reconocido expresamente por los artículos 17.1 del Pacto

Internacional de Derechos Civiles y Políticos, y 11.2 de la Convención Americana sobre Derecho Humanos. El primero de estos preceptos dispone: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". El artículo 11.2 de la Convención Americana es casi idéntico.

El mismo párrafo noveno del artículo 16 establece la posibilidad de que la autoridad judicial federal autorice la intervención de cualquier comunicación privada. Esta autorización debería haber quedado prevista como una *excepción* frente a la regla general de la inviolabilidad de las comunicaciones privadas. Sin embargo, la redacción del párrafo no resulta precisa, pues no regula la autorización de la intervención como una verdadera excepción, sino como una muy amplia posibilidad sujeta a lo que dispongan las leyes ordinarias.

El párrafo noveno sólo indica que pueden solicitar la autorización: 1) la autoridad federal que faculte la ley, y 2) el titular del Ministerio Público de la entidad federativa correspondiente: Inicialmente se estimó que por la amplitud de la redacción del párrafo, dentro de la expresión "autoridad federal que faculte la ley" pueden quedar no sólo los agentes del Ministerio Público Federal, sino prácticamente cualquier autoridad federal, con la única condición de que la faculte la ley para tal fin, lo que se descartó con motivo de que es al Ministerio Público a quien corresponde la investigación y persecución de los delitos. La facultad para otorgar la autorización se atribuye exclusivamente a la "autoridad judicial federal", es decir, a los órganos del Poder Judicial de la Federación.

El tema del derecho a la no intromisión de las comunicaciones privadas es un punto álgido en el Internet, Nora Cherñavsky sostiene que las conductas y contenidos a restringir deben estar tipificadas legalmente, haciendo compatible las conductas sin valor con el mayor y más amplio de los respetos a la libertad de expresión y al derecho –hoy fundamental– de tener acceso a la información, con lo que a su juicio se pretende que el ciudadano visualice al Estado como aliado en la lucha contra los riesgos que sufren los beneficios de la expansión de la actividad informática y no como una amenaza a sus derechos a la intimidad y libertad.[11]

[11] Cherñavsky, Nora, "Libertad de expresión por Internet. Límites éticos y constitucionales", *AR: Revista de Derecho Informático*, núm. 064, noviembre de 2003, http://www.alfa-redi.org/rdi-artículo.shtml?x=269.

A nuestra apreciación y desde el entorno jurídico que rige a nuestro país la investigación de los delitos en el Internet es problemático no tan solo por los aspectos de transterritorialidad y trasnacionalidad ya comentadas, sino también porque la Constitución reconoce como un derecho subjetivo público la no intervención de las comunicaciones privadas, entiéndase no como un obstáculo al precitado derecho, más bien, nos referimos a la dificultad de que el Ministerio Público en su afán persecutorio logre llevar a cabo las pesquisas necesarias.

Ciertamente, de modo indefectible y sólo en aquéllos casos que lo faculte la ley ordinaria, el Ministerio Público podrá solicitar a la autoridad judicial federal la autorización de intervenir las comunicaciones privadas, lo que el legislador ordinario reservó en aquéllos casos de que exista delincuencia organizada, en que el Procurador General de la República o el titular de la Unidad Especializada lo consideren necesario, con expresión del objeto y necesidad de la intervención, y que los indicios hagan presumir fundadamente que en los hechos investigados participe algún miembro de la delincuencia organizada.

La medida anterior tiene como objeto proteger el derecho a la comunicación privada, reservándose la intromisión legal sólo en aquéllos casos en que existan indicios de la existencia de delincuencia organizada; consecuentemente, no existe manera de que el Estado a través de la representación social persiga aquéllos delitos que podrían considerarse no graves por la legislación penal, lo que a nuestro modo de ver propicia impunidad, dicho de otro modo, los ilícitos más comunes como son los desvíos patrimoniales a través de Internet, no podrían obtenerse datos provenientes de una intromisión legal a las comunicaciones privadas, en un contexto similar se conduce Marcelo A. Riquert al señalar la necesidad de actualizar la legislación en relación con los abusos relacionados con la informática que deben ser combatidos con medidas jurídico penales.[12]

A modo de ejemplo, el fenómeno de robo de identidad, se ha expandido como plaga, en las estadísticas de la Comisión Federal de Comercio de los Estados Unidos de Norte América, sólo en ese país en los últimos cinco años

[12] Riquert, Marcelo A., "Estado de la legislación contra la delincuencia informática en el Mercosur", *AR: Revista de Derecho Informático*, núm. 116, marzo de 2008, http:www.alfa-redi.org/rdi-artículo.shtml?x=10136.

se han robado cuentas bancarias y tarjetas de crédito que han afectado a veintisiete millones de personas, casi el cinco por ciento de los adultos norteamericanos, con un perjuicio de cincuenta mil millones de dólares.[13]

Lo anterior refleja la existencia de delitos informáticos que sin necesidad de revestir la gravedad que requiere la ley penal, producen una afectación significativa en el detrimento del patrimonio de muchas personas, por lo que es un verdadero reto tratar de instrumentar los mecanismos necesarios para disminuir la incidencia delictiva a través de Internet.

IV. Delitos informáticos

1. *Delitos informáticos, una aproximación*

Por delito informático, suele entenderse toda aquélla conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.

Organismos internacionales como la OCED, lo define como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.[14]

Para Julio Téllez Valdez, los delitos informáticos son aquéllas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico).[15]

El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.[16]

[13] *Idem*.

[14] López Betancourt, Eduardo, *Delitos en particular*, México, Porrúa, 2004, p. 270.

[15] Téllez Valdés, Julio, *Derecho informático*, 3ª. ed., México, McGraw-Hill, 2004, p. 163.

[16] *Ídem*.

Para Gabriel Andrés Campoli, los delitos informáticos son aquéllos en los cuales el sujeto activo lesiona un bien jurídico que puede o no estar protegido por la legislación vigente y que puede ser de diverso tipo por medio de la utilización indebida de medios informáticos, agrega que delitos electrónicos o informáticos electrónicos, son una especie del género delitos informáticos, en los cuales el autor produce un daño o intromisión no autorizada en equipos electrónicos ajenos y que a la fecha por regla general no se encuentran legislados, pero que poseen como bien jurídico tutelado en forma específica la integridad de los equipos electrónicos y la intimidad de sus propietarios.[17]

En relación con lo anterior estimamos que deben hacerse algunas precisiones en torno a los elementos del delito; con el fin de exponer las particularidades del delito informático desde la perspectiva actual; así, desde la óptica de Díaz-Aranda,[18] en los cuatro sistemas del delito que fueron desarrollados en Alemania (clásico, neoclásico, finalista y funcionalista) se ha considerado que la conducta por si misma es el presupuesto o uno de los elementos del delito; sin embargo ello conduce a que en todo momento se analice la existencia de conductas y de resultados para después volver a analizarla para saber si esta prohibida en la ley; es decir, si es una conducta- típica; por el contrario, cuando se intuye que un hecho puede ser constitutivo de delito, lo primero que se hace acudir a las normas para saber si eso está o no prohibido en la ley penal, lo que conduce a que el análisis no inicie con una conducta prejurídica sino con el indicio de un hecho descrito en la ley como prohibido y eso es la tipicidad entendida como juicio de adecuación de la conducta al tipo.

2. *La antijuridicidad*

En el elemento de la antijuridicidad el objetivo es establecer si la conducta prohibida por la legislación es contraria al orden jurídico en general, y por ello al hecho típico y antijurídico se le denomina "injusto".

Por el contrario, si el hecho típico está amparado por alguna causa de justificación ya no hay delito. De ahí la conocida frase: "el tipo es un puro

[17] Campoli, Gabriel Andrés, "Hacia una correcta hermenéutica penal delitos informáticos vs. delitos electrónicos" *AR: Revista de Derecho Informático* núm. 048, julio de 2002, http://www.alfa-redi.org/rdi-artículo.shtml?x=1480.

[18] Díaz-Aranda Enrique, *Teoría del delito*, México, Straf, 2006, p. 203.

objeto de la valoración, mientras que la valoración de ese objeto se produce en el marco de la categoría de la antijuridicidad".

En la conducta-típica, la preocupación natural de la doctrina, es ocuparse de delimitar si la conducta encuadra en el tipo y podría ser particularmente considerada como una conducta prohibida para el derecho penal, en contrapartida, en la categoría de la antijuridicidad se analiza si esa conducta prohibida se justifica de cara a todo el orden jurídico por las circunstancias materiales que concurrieron en el momento de su realización o si, por el contrario, se constata que el hecho resulta un injusto (conducta-típica y antijurídica).

Las precisiones anteriores servirán como punto de partida para establecer el terreno en que deben ubicarse los delitos informáticos, puesto que en su mayoría resultan de nueva creación por el legislador y por lo mismo requieren de una atención especial, ya que en algunos casos su descripción legal no corresponde precisamente a las conductas que originalmente se tuvo presentes para sancionar, errores que en ocasiones por la mala integración de la averiguación previa, posteriormente conducen a un resultado adverso al no lograrse el enjuiciamiento y dictado de la sentencia correspondiente.

3. *La culpabilidad*

La culpabilidad es la tercera categoría y último escalón de la teoría del delito, consiste en un juicio sobre el autor mediante el cual se determina si se le puede reprochar el haberse comportado de manera contraria a lo que establece el orden jurídico.

La culpabilidad se conforma de tres elementos: la imputabilidad del sujeto, su conciencia sobre la antijuridicidad de la conducta y la ausencia de causas excluyentes de la culpabilidad.

De modo breve, cabe señalar que en relación con el primer elemento (imputabilidad) es necesario que exista una capacidad psíquica del sujeto para comprender el hecho y su trascendencia, para ello se requiere que ese juicio lo pueda realizar quien es mayor de edad y por ello se le considere como imputable, y en el caso de que sea mayor de dieciocho años que no sufra de deficiencias mentales permanentes o transitorias.

Por cuanto a la característica descrita, cabe destacar que el artículo 18, párrafo cuarto, de la Constitución Federal, cobra especial relevancia con

motivo de que el manejo de las PC resulta sumamente asequible a los menores de edad, los cuales con independencia de que carezcan de una alta preparación tecnológica se desempeña en muchas ocasiones con mayor comodidad y fluidez que los mismos adultos, lo que propicia que se deberá tener especial atención por cuanto a la sujeción de dichos menores infractores al procedimiento que establezcan las correspondientes leyes ordinarias.

En Cuba se han llevado a cabo estudios sobre el tipo de sujetos acusados y con mayor incidencia en delitos de informática en el que han advertido que la edad promedio es entre treinta y treinta y nueve años de edad.[19] También es de resaltar que se ha configurado que la incidencia es baja en este tipo de delitos, lo que probablemente obedezca a las carencias tecnológicas, puesto que hace unos cuantos días se dio la apertura del teléfono celular en dicho país, como así se informó en el noticiero Primero Noticias de Televisa el día dieciséis de abril de año en curso.

Debe señalarse además que a los elementos que se requieren para la acreditación del delito, surge recientemente un nuevo punto de controversia.

Cierto, hace poco más de un año se aprobaron modificaciones a la Constitución Federal, entre las que nos interesa, para el presente estudio, la modificación al artículo 16, párrafo segundo, constitucional y que atiende a los requisitos necesarios para el libramiento de una orden de aprehensión, el que en comparación con el anterior texto se suprime la frase "cuando menos" (cuando menos con pena privativa de libertad…) y se dice que deben obrar datos que establezcan que se ha cometido ese hecho (hecho delictivo) y que exista la posibilidad de que el indiciado lo cometió o participó en su comisión.

La frase "cuando menos", puede que sea innecesaria al referirse que la sanción del delito correspondiente debe ser privativa de la libertad personal; ya que aún cuando exista la posibilidad de pena alternativa, aún en estos casos se entiende que habrá lugar a la orden de comparecencia, además de que actualmente ya no existe la pena de muerte en México, la que fue abrogada en el año de 2005, por lo que ya no es necesario tal frase.

El párrafo en cuestión precisa que cuando obren datos que "establezcan" que ha cometido el hecho, estimamos que la palabra establecer no es clara

[19] Cordobés, Enrique, "Características generales de la criminalidad informática en Cuba", *AR: Revista de Derecho Informático*, núm. 098, septiembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=7178.

ni tampoco sinónimo de acreditar, lo que puede dar lugar a confusiones y que perjudiquen a una persona en el momento de que se emita un mandamiento de captura.

La supresión del concepto cuerpo del delito cambia por el de hecho delictivo, éste término complica de algún modo la dogmática jurídica que se ha manejado históricamente, aunque consideramos que es un término más sencillo o de lenguaje coloquial y que desde luego difiere de la connotación doctrinal de "cuerpo del delito" o "tipo penal"; ninguna legislación fue uniforme al definir el cuerpo del delito y, por ende, cambiarlo por hecho delictivo resulta más conveniente; se comprende también que doctrinariamente lo que se debe acreditar son los elementos objetivos del tipo penal, los que se perciben con los sentidos, los elementos materiales; y que esto deberá desarrollarse a través de la ley secundaria.

Además, cambia el término *probable responsabilidad*, por *probable comisión* o *participación del delito*. A nuestro modo de ver, el cambio obedece a querer ser más claros o precisos en cuanto a la conducta del imputado; o es autor material o coautor o cómplice, ello no afecta en gran medida la modificación, aunque tal aspecto también deberá ser objeto acucioso de estudio.

Concluimos que de la forma en que esta redactado el artículo 16, párrafo segundo, constitucional, el dictado de la orden de aprehensión será más sencillo, con menos requisitos que los que ahora se exigen, y la motivación de la resolución no será tan rigorista, pues no se exigirá la comprobación de los elementos del tipo penal, sino las pruebas que acrediten el hecho delictuoso y la comisión o participación del indiciado.

La reforma constitucional en comento consideramos que concretamente en materia de delitos informáticos causará un gran impacto al hacer más sencillo el establecimiento de los datos necesarios para el libramiento de una orden de aprehensión; sin embargo, estimamos que también es un arma de doble filo, puesto que eventualmente podrán emitirse ordenes de aprehensión sin la certeza jurídica de que exista la totalidad de los elementos necesarios para ello.

4. *Naturaleza jurídica del derecho informático*

El derecho informático, surge como una nueva rama del Derecho, como consecuencia de las siguientes consideraciones de que se requiere una regularización de los bienes informacionales, porque la información como

producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico; es necesaria la protección de datos personales. Debido al atentado sufrido a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas; el flujo de datos transfronterizos. Sobre el favorecimiento de restricción en la circulación de datos a través de fronteras nacionales; la protección de programas. Como solución a los problemas mas provocados por la llama piratería o pillaje de programas de cómputo; los delitos informáticos en sentido amplio. Así como la comisión de verdaderos actos ilícitos en los que se tenga en la computadora un instrumento o fin.[20]

Evidentemente, el desarrollo de nuevos ordenamientos destinados a regular el flujo de información a través de los sistemas computacionales, tendrá incidencia en el ámbito penal.

La Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

1. 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.
2. Falsificaciones informáticas
   a) Utilizando sistemas informáticos como objetos.
   b) Utilizando sistemas informáticos como instrumentos.
3. Daños o modificaciones de programas o datos computalizados.
   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.[21]

[20] López Betancourt, Eduardo, *op. cit*. p. 271.
[21] *Ídem*.

5. Breve reseña histórica del delito informático

La concepción de los delitos informáticos en nuestro país tendrá escasos diez años; sin embargo, en los Estados Unidos de Norteamérica, la primera propuesta de legislar con este respecto, se presentó en 1977 por el senador Ribicoff en el Congreso Federal.[22]

Años después, en 1983 en París, la OECD designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. El dictamen de esta organización, recomendó a los países miembros la modificación de su legislación penal, de forma que se integraran los nuevos delitos informáticos.

En 1989, el Consejo de Europa convocó a otro comité de expertos, que en la Recomendación emitida el 13 de septiembre de ese año, presentaron una lista mínima de los delitos que debían necesariamente agregarse a las legislaciones de cada país miembro, junto con una lista opcional.

También se llegó a discutir sobre estos temas en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado de Montreal en 1990, en el Octavo Congreso Criminal de las Naciones Unidas celebrado en el mismo año, y en la Conferencia de Wurzburgo, en Alemania, en 1992.

En 1996, se estableció por el Comité Europeo para los Problemas de la Delincuencia, un nuevo comité de expertos para que abordaran el tema de los delitos informáticos.

Con el fin de combatir los delitos informáticos, sobre todo los cometidos a través de las redes de telecomunicaciones, en Internet, como pueden ser las transacciones de fondos ilegales, la oferta de servicios ilegales, la violación de los derechos de autor, así como también los delitos que violan la dignidad humana y la protección de los menores, se encargó la tarea de elaborar un borrador del instrumento legal obligatorio al recién formado "Comité Especial de Expertos sobre Delitos relacionados con el empleo de Computadoras".

El veintitrés de noviembre de dos mil uno, el Consejo de Ministros de Europa, compuesto por los ministros del interior de los estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón, firmaron en Budapest, la convención sobre delitos informáticos, cuyos objetivos fundamentales fueron los siguientes:

[22] *Ídem*. p. 274.

1. Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.
2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas, y
3. Establecer un régimen dinámico y efectivo de cooperación internacional.[23]

En nuestro sistema jurídico se incluyó a los delitos informáticos justamente con las reformas que se publicaron en el *Diario Oficial de la Federación* el diecisiete de mayo de mil novecientos noventa y nueve.

Los novedosos ilícitos se ubicaron dentro de Título Noveno del código punitivo federal, al que se denominó "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática".

Resulta de interés al desarrollo de estas líneas las causas medulares que dieron origen a la exposición de motivos de la reforma, al considerarse que la iniciativa propone adicionar un capítulo al código penal para sancionar al que sin autorización acceda a sistemas y equipos informáticos protegidos por algún mecanismo de seguridad, con el propósito de conocer, copiar, modificar o provocar la pérdida de información que contenga, por lo que se pretende tutelar la privacidad y la integridad de la información.

Lo anterior refleja que para el legislador fue de suma importancia proteger el acceso no autorizado a computadoras o sistemas electrónicos, la destrucción o alteración de información, el sabotaje por computadora, la intercepción de correo electrónico, el fraude electrónico y la transferencia ilícita de fondos, ilícitos que no son privativos de nuestro entorno, sino que suceden con frecuencia en el ámbito internacional y que constituyen, desde luego, un grave problema ante la revolución tecnológica que ha rebasado las estructuras de contención, control y vigilancia por parte de los Estados.

En un sentido similar, se conduce Erika Tinajeros Arce al señalar que el uso de las técnicas informáticas, ha creado nuevas posibilidades del uso indebido de las computadoras, lo que ha propiciado a su vez la necesidad de

[23] Muñoz Esquivel, Oliver, "La convención sobre delitos informáticos", *AR: Revista de derecho informático*, núm. 042, enero de 2002, http://www.alfa-redi.org/rdi-artículo.shtml?x=1582

regulación por parte del Derecho. Añade que el sabotaje informático es el acto mediante el cual se logra inutilizar, destruir, alterar o suprimir datos, programas e información computarizada, sus inicios se dieron en los laboratorios del Instituto de Massachussets en 1960, al crearse un dispositivo informático destructivo mediante la utilización del lenguaje assambler.[24]

El diverso delito de revelación de secretos que establece el artículo 211 del enunciado Código Penal Federal, prevé sanción de uno a cinco años, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público, o cuando el secreto revelado o publicado sea de carácter industrial, el subsecuente numerario 211 Bis, de dicho ordenamiento legal, dispone que a quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión.

Tales ilícitos también pueden considerarse como un fin en tratándose del uso de computadoras, sobre todo cuando se trata de información de tipo industrial, en relación con el ordinal 211 Bis, de la ley del enjuiciamiento penal federal, la Primera Sala del más alto Tribunal de Justicia de la Nación, ha establecido de que el vocablo "indebidamente" empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, el segundo, porque su sentido puede fijarse desde el punto de vista jurídico y determinar cuando la conducta es indebida para considerarse delictuosa. Además, el hecho de que el Código Penal Federal no contenga un anunciado especial que desentrañe el significado de ese elemento normativo, lo cual se entiende por constituir un elemento de valoración jurídica, no implica infracción a la citada garantía, pues, se trata de un concepto cuyo contenido resulta claro tanto en el lenguaje común como en el jurídico.[25]

[24] Tinajeros Arce, Erika, "Nuevas formas de delinquir en la era tecnológica: Primeras observaciones sobre espionaje, fraude y sabotaje informático", *AR: Rrevista de derecho informático*, núm. 098, septiembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=7182.

[25] Tesis 1ª.LXXXBIII/2005, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXII, agosto de 2005, p. 302.

6. *Clasificación de los delitos informáticos*

Tal parece que el eje central de los delitos informáticos se da en la manipulación de los datos de entrada, programas y salidas de computadoras, así como la falsificación de los sistemas informáticos, y el espionaje de información, esa conjunción de elementos produce en el sujeto pasivo un daño en su patrimonio; por ello estimamos que los ilícitos cometidos a través de Internet en su mayoría causan una afectación al patrimonio de los pasivos.

A modo de citar un ejemplo en el Código Penal brasileño se tipificó el delito de inserción de datos falsos en sistemas de información y el delito de modificación o alteración no autorizada de sistemas de información de la administración pública; tal reforma se dio como consecuencia de la intromisión de empleados públicos al acceso del sistema informatizado del gobierno del estado de Río Grande Donarte.[26]

Aunque existen también delitos que se cometen a través de Internet y causan afectación a bienes jurídicos de diversa naturaleza, como acontece con los antijurídicos de pornografía infantil.

A. Delitos patrimoniales

De acuerdo con la información que proporciona Banamex, Citybank, el fraude electrónico causa una gran afectación a los usuarios de la banca, siendo el país de los Estados Unidos el principal blanco de dichos ataques, con un cincuenta y dos por ciento, los ataques informáticos se generan en contra de los clientes y no en contra de la institución crediticia, lo que obedece a los sistemas de protección que gozan las instituciones bancarias, tales ataques se llevan a cabo a través de dos programas que se denominan: Phising y Pharming, el propósito de esos programas es hacerse de los recursos del usuario de la banca, aprovechándose de dos factores básicos que toman en consideración los defraudadores, los cuales son el nivel cultural del usuario y la natural curiosidad del ser humano.[27]

[26] Ramos Junior, Hélio Santiago, "Delitos cometidos contra la seguridad de los sistemas de informaciones de la administración pública brasileña", *AR: Revista de Derecho Informático*, núm. 115, febrero de 2008, http://www.alfa-redi.org/rdi-artículo.shtml?x=10131.

[27] Videoconferencia "*Delitos cibernéticos*", tema citado, p. 21

Ante los ataques de los defraudadores cibernéticos se han instrumentado sistemas básicos de protección que debe tener cualquier usuario de Internet, entre los cuales destacan:

1. Tener una herramienta antivirus vigente y actualizada.
2. Poseer herramientas antiintrusos.
3. Tener un firewall personal.
4. Tener autorizados parches de seguridad, y
5. Controlar las entradas y salidas de las unidades usb y disquetes para evitar las descargas de impresiones fotográficas, entre otras.

Además, se recomienda lo siguiente:

a) No compartir el e-mail.
b) No enviar información confidencial.
c) No dar clic a ligas adjuntas a e-mailes, y
d) Proteger siempre el equipo con antivirus.

A los esfuerzos de la citada institución bancaria se añade la creación de la unidad ICRAI cuyo objetivo es el análisis de los sistemas informáticos a través de cómputo forense, pueden estudiar los registros anteriores de las computadoras, así como también llevan a cabo la revisión de las computadoras en el momento en que se están utilizando.

Tales medidas son de gran ayuda para detectar los fraudes cibernéticos, lo que aunado a la reciente reforma al artículo 52 de la Ley de Instituciones de Crédito, en la que se establece que las instituciones de crédito pueden suspender o cancelar el trámite de operaciones en los casos en que su clientela pretenda realizar el trámite de operaciones mediante el uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, cuando cuenten con elementos suficientes para presumir que los medios de identificación pactados para tal efecto han sido utilizados en forma indebida, resulta sin lugar a duda de un gran apoyo legal al usuario desprotegido en el mundo del Internet.

B. Delitos de pornografía

El Código Penal Federal en su artículo 201 Bis establece el tipo descriptivo consistente en que 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.

El legislador también dispuso que al que fije, grabe imprima datos de exhibicionismo corporal, lascivos o sexuales en que participen uno o más menores de dieciocho años, se le impondrá la pena de diez a catorce años de prisión y de quinientos a tres mil días multa. La misma pena se impondrá a quien con fines de lucro o sin el, elabore, reproduzca, venda, arriende, exponga, publicite o transmita el material a que se refieran las acciones anteriores.

De igual manera se establece la pena de prisión de ocho a dieciséis años, a quien por sí u a través de terceros, dirija administre o supervise cualquier tipo de asociación delictuosa con el propósito de que se realicen las conductas previstas en los dos párrafos anteriores con menores de dieciocho años.

El mismo precepto en su parte define como pornografía infantil, la representación sexualmente explicita de imágenes de menores de dieciocho años.

Como se puede apreciar en nuestro país si se encuentra sancionada por la ley penal la pornografía infantil mediante anuncios electrónicos. El problema a dilucidar en este caso, es que el órgano encargado de investigar y perseguir las conductas delictuosas (Ministerio Público) esté en aptitud de iniciar la averiguación previa con el suficiente soporte técnico, puesto que en el mayor de los casos, se debe enfrentar bandas que conforman delincuencia organizada y que pueden estar ubicados físicamente en un diverso país, como ya se ha comentado en páginas anteriores, a lo que se suma el derecho establecido en la Constitución de no intervenir en las comunicaciones privadas, que se traduce en que se requiere autorización judicial por parte de un Juez de Distrito para escuchar y ver tales imágenes a que accede un usuario de Internet.

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.[28]

[28] 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.

En ese mismo tenor, se expresa Graciela M. Landa Durán, al establecer que entre los delitos que se pueden cometer por medios tecnológicos, destacan, entre otros los delitos contra la libertad e indemnidad sexuales cometidos por medios electrónicos, particularmente la difusión de pornografía infantil a través de la red.[29]

La misma autora, expresa que en España se ha legislado en relación con las infracciones relativas al contenido que incluyen múltiples conductas realizadas sobre materiales de pornografía infantil, en el que se incluyen conductas de producción ofrecimiento, difusión, transmisión o procuración para otro, por medio de un sistema informático de pornografía infantil, también se extiende la incriminación a la obtención para sí mismo de estos materiales mediante un sistema informático o la mera posición del material de un sistema informático o de almacenamiento de datos informáticos.

C. Delincuencia organizada

El legislador estableció que en aquéllos casos de la averiguación previa de alguno de los delitos a que se refiere la ley contra la delincuencia organizada, o durante el proceso respectivo, el Procurador General de la República o el titular de la Unidad Especializada consideren necesaria la intervención de comunicaciones privadas, lo solicitarán por escrito al Juez de Distrito, expresando el objeto y necesidad de la intervención, los indicios que hagan presumir fundadamente que en los delitos investigados participa algún miembro de la delincuencia organizada, así como los hechos, circunstancias, datos, y demás elementos que se pretenda probar.

De especial interés fue para el legislador que en las solicitudes de intervención deberán señalar, además, la persona o personas que serán investigadas; la identificación del lugar o lugares donde se realizarán; el tipo de comunicación privada a ser intervenida; su duración; y el procedimiento y equipos para la intervención y, en su caso, la identificación de la persona a cuyo cargo está la prestación del servicio a través del cual se realiza la comunicación objeto de la intervención.

Se establece además que podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o

[29] Landa Duran, Graciela M., "Los delitos informáticos en el Derecho penal de México y España", *Revista del Instituto de la Judicatura Federal*, núm. 24, 2007, p. 248.

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.

En relación con este tópico, el Cuarto Tribunal Colegiado en Materia Penal del Primer Circuito,[30] estableció que la limitación establecida por el precepto 16 Constitucional en relación con la figura de intervención de comunicaciones privadas, que el bien jurídico de la infracción penal por intervención de comunicaciones privadas cometidas por servidores públicos recae en el interés común, pues la finalidad perseguida con la incursión de la figura de la intervención de comunicaciones privadas previa autorización judicial, fue precisamente la de proteger a la colectividad contra el constante incremento del crimen organizado, de ahí que la lesión por el ilícito en comento recae en la sociedad, convirtiéndose así en sujeto pasivo de la infracción punitiva, puesto que la salvaguarda de la seguridad y privacidad de las comunicaciones, como se dijo, encuentran su limitante en la satisfacción del interés común de la sociedad, quien es la interesada en que el derecho a la privacía no sea violable sino sólo en los casos permitidos por la ley.

V. Conclusiones

1. Se requiere un manual de ética que como política de una sana relación en el uso de Internet, se instrumente y participe a cada usuario para eliminar en lo posible conductas delictuosas.
2. El legislador debe estar consciente de la extraterritorialidad y transnacionalidad de los delitos que se cometen a través de Internet; por ello, el conocimiento de las conductas delictuosas cometidas a través de la red debe corresponder a los órganos del Poder Judicial de la Federación.
3. Se debe instrumentar una policía cibernética eficaz y altamente preparada tecnológicamente para investigar y perseguir los delitos que se cometen en Internet.

[30] Tesis I.4º.P.21P *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XVIII, julio de dos mil tres, p. 1146.

4. Sería conveniente aglutinar los delitos informáticos en una ley especial.
5. La reforma al artículo 16, párrafo segundo, Constitucional, simplifica los requisitos para el dictado de una orden de aprehensión, lo que propiciará el libramiento de órdenes de captura de modo más ligero en tratándose de delitos informáticos.

VI. Glosario

Blindar. Protección adicional a un instrumento.

Ciberespacio. Término creado por William Gibson en su novela fantástica *Neuromanser*, del año 1984 para describir el mundo de las computadoras y la sociedad creada en torno a ellas.

FTP. Protocolo de transferencia de ficheros, que permite al usuario de un sistema acceder a, y transferir desde, otro sistema de una red.

Host. Anfitrión, albergar, hospedar.

Internet. Red de telecomunicaciones iniciada en el año de 1969 en los Estados Unidos, con objetivos militares, industriales y universitarios, posteriormente se dio a conocer a todo el mundo, teniendo así un desarrollo impresionante, equiparable a la tercera revolución del mundo, la primera fue el desarrollo de la agricultura y la segunda la revolución industrial.

PC. Computadora personal con funciones cada vez más sofisticadas.

Servidor. Sistema que proporciona recursos (servidores de ficheros, servidores de nombres). En Internet se utiliza para designar aquéllos sistemas que proporcionan información a los usuarios de la red.

Spam. Envío indiscriminado y no solicitado de publicidad a través de correo electrónico.

Usuario. Es el nombre intelegible que identifica al usuario de un sistema o red.

Web. Servidor de información www. Se utiliza también para definir el universo www en su conjunto.

Referencias

Bibliográficas

Barriuso Ruiz, Carlos, *La contratación electrónica*, Madrid, Dykison, S.L., 2002

López Betancourt, Eduardo, *Delitos en particular*, Porrúa, México, 2004.

Márquez Romero, Raúl, *Constitución Política de los Estados Unidos Mexicanos, comentada y concordada*, tomo V. Porrúa, México, 2004.

Palomar de Miguel, Juan, *Diccionario para juristas*, Porrúa, México, 2000.

Téllez Valdés Julio *Derecho informático*, 3ª edición, McGraw-Hill Interamerica, México, 2004.

Zabale, Ezequiel, "La competencia en materia de acciones civiles o penales derivadas del uso de la red Internet", *Derechos informáticos*, Argentina, 2002.

Hemerográficas

Batiz Álvarez, Verónica, "Panorama General del Marco Jurídico en Materia Informática en México", *AR: Revista de Derecho Informático*, núm. 066, enero de 2004, http://www.alfa-redi.org/rdi-artículo.shtml?x=1246.

Campoli, Gabriel Andrés, "Los dos delitos más comunes y controversiales cometidos por medios informáticos: clonación de tarjetas de crédito y phishing o transferencias electrónicas ilegítimas", *AR: Revista de Derecho Informático*, núm. 101, diciembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=8083.

————, "Pasos hacia la reforma penal en materia de delitos informáticos en México", *AR: Revista de Derecho Informático*, núm. 079, febrero de 2005, http://www.alfa-redi.org/rdi-artículo.shtml?x=974.

————, "Hacia una correcta hermenéutica penal- delitos informáticos vs. Delitos electrónicos", *AR: Revista de Derecho Informático*. núm. 048, julio de 2002, http://www.alfa-redi.org/rdi-artículo.shtml?x=1480.

Cordobés, Enrique, "Características Generales de la Criminalidad Informática en Cuba", *AR: Revista de Derecho Informático*, núm. 098, septiembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=7178.

Cherñavsky, Nora, "Libertad de expresión por Internet. Límites éticos y constitucionales", *AR: Revista de Derecho Informático*, núm. 064, noviembre de 2003, http://www.alfa-redi.org/rdi-artículo.shtml?x=269.

Farinella, Flavio, "Algunas notas sobre el Spamming y su regulación", *AR: Revista de Derecho Informático*, núm. 094, mayo de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=6102.

Muñoz Esquivel. Oliver, "La convención sobre delitos informáticos", *AR: Revista de Derecho Informático*, núm. 042, enero de 2002, http://www.alfa-redi.org/rdi-artículo.shtml?x=1582.

Ramos Júnior, Hélio Santiago, "Delitos cometidos contra la seguridad de los sistemas de informaciones de la Administración Pública Brasileña", AR: Revista de Derecho Informático, núm. 115, febrero de 2008, *http://www.alfa-redi.org/rdi-artículo.shtml?x=10131*.

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.

Riquert, Marcelo A., "Estado de la Legislación Contra la Delincuencia Informática en el Mercosur", *AR: Revista de Derecho Informático*, núm. 116, marzo de 2008, http://www.alfa-redi.org/rdi-artículo.shtml?x=10136.

Tinajeros Arce, Erika, "Nuevas Formas de Delinquir en la Era Tecnológica: Primeras Observaciones Sobre Espionaje, Fraude y Sabotaje Informático", *AR: Revista de Derecho Informático*, núm. 098, septiembre de 2006, http://www.alfa-redi.org/rdi-artículo.shtml?x=7182.

Valle Puga González, Paula, "Responsabilidad de los prestadores de servicios de la sociedad de la información", *AR: Revista de Derecho Informático*, núm. 030, enero de 2001, http://www.alfa-redi.org/rdi-artículo.shtml?x=5726.

Cibergráficas

http://ciberhabitat.gob.mx/noticias/mar2007.htm, 15 de abril de 2008.