

# **QUE REFORMA, ADICIONA Y DEROGA DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL, DEL CÓDIGO FEDERAL DE PROCEDIMIENTOS PENALES, DE LA LEY FEDERAL CONTRA LA DELINCUENCIA ORGANIZADA Y DE LA LEY DE LA POLICÍA FEDERAL PREVENTIVA, EN MATERIA DE DELITOS CIBERNÉTICOS Y DE DELITOS CONTRA MENORES**

La que suscribe, Sheyla Fabiola Aragón Cortés diputada del Estado de México por la quinta circunscripción de la LIX Legislatura del H. Congreso de la Unión, integrante del grupo parlamentario del Partido Acción Nacional, con fundamento en los artículos 71, fracción II, 72 y 73, fracción XVI, de la Constitución Política de los Estados Unidos Mexicanos; 26 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; 55, fracción II, 56, 60 y 64 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos; solicito se turne a las Comisiones de Comunicaciones y de Justicia y Derechos Humanos para su dictamen y posterior discusión en el Pleno de esta H Asamblea, la siguiente iniciativa con proyecto de decreto que adiciona, reforma y deroga diversas disposiciones del Código Penal Federal, Código Federal de Procedimientos Penales, Ley Federal Contra la Delincuencia Organizada y Ley de la Policía Federal Preventiva; relativas a los delitos cibernéticos y delitos contra menores, con base en la siguiente

## **Exposición de Motivos**

Los motivos que llevan a la presentación de esta iniciativa de reforma y adiciones al Código Penal Federal, al Código Federal de Procedimientos Penales, a la Ley Federal contra la Delincuencia Organizada y la Ley de la Policía Federal Preventiva cuentan con los siguientes:

### **Antecedentes**

I. En 1996 la Organización de las Naciones Unidas emitió la Declaración de Estocolmo contra la Explotación Sexual Infantil con Fines Comerciales, la cual México firmó como Estado Parte, comprometiéndose a establecer medidas legislativas con el fin de evitar la pornografía y prostitución infantiles.

II. En marzo de 1999 la Organización de los Estados Americanos (OEA), dentro del marco de la Segunda Reunión de Ministros de Justicia o Procuradores Generales de las Américas, recomendaron integrar un grupo de expertos intergubernamentales sobre delito cibernético para evaluar la actividad delictiva, la legislación, la política y las prácticas nacionales contra esta actividad, así como establecer mecanismos de cooperación entre las naciones del continente para perseguir este mal.

III. El 17 de mayo de 1999 se publicó en el Diario Oficial de la Federación, la modificación al Título Noveno del Código Penal Federal con el nombre de "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática" y se adicionó un Capítulo II con siete nuevos tipos penales, los llamados equipos informáticos.

IV. El 29 de mayo de 2000 se publicaron en el Diario Oficial diversas reformas y adiciones en materia de comercio electrónico al Código Civil para el Distrito Federal en materia común y para toda la República en materia federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.

V. En el año 2000 la Secretaría de Seguridad Pública a través de la Policía Federal Preventiva creó la Unidad de Policía Cibernética y Delitos contra Menores, siendo la primera policía en su tipo en México cuyas actividades incluyen el patrullaje de la Internet, pornografía infantil, atención a fraudes computacionales, análisis de daños a sistemas, detección de sitios de alto riesgo criminal, tráfico de drogas, armas y terrorismo.

VI. En junio de 2002 se publicaron en el Diario Oficial reformas y adiciones a diversas disposiciones del Código de Comercio, en materia de firma electrónica, para su regulación y efectos jurídicos en las transacciones y certificaciones electrónicas.

VII. El 9 de diciembre de 2002 inicia funciones el Grupo de Coordinación Interinstitucional para Combatir los Delitos Cibernéticos (DC México), integrado por el gobierno federal y los gobiernos estatales, instituciones académicas, proveedores de servicio de Internet y organizaciones civiles y privadas.

VIII. Del 27 al 30 de enero de 2004 este H. recinto fue sede del Foro Legislativo en Materia de Delitos Cibernéticos organizado conjuntamente con la Organización de Estados Americanos (OEA) y el Departamento de Justicia de los Estados Unidos de América, con la asistencia de representantes de diversos países de Centro y Sudamérica.

IX. El 10 marzo de 2004 mediante Punto de Acuerdo de la Comisión Permanente del Congreso de la Unión, se exhortó a la Secretaría de Relaciones Exteriores a iniciar las gestiones para la adhesión de México al Convenio del Consejo de Europa sobre Cibercrimen.

X. El 23 de marzo de 2004 el Subgrupo Jurídico y de Consultoría Legislativa de Grupo DC México entregó a la Comisión de Comunicaciones de la Cámara de Diputados una propuesta de modificaciones a diversos ordenamientos legales, para ser estudiadas con el fin de elaborar una iniciativa al respecto.

XI. Por oficio recibido el 29 de abril de 2004 en este recinto, la Cámara de Senadores informa del Dictamen sobre los Delitos Cibernéticos aprobado por el pleno.

XII. A través de oficio recibido el 14 de julio de 2004 en la Comisión Permanente, el Gobierno Federal a través de la Secretaría de Relaciones Exteriores respondió al Punto de Acuerdo referido en el antecedente IX.

XIII. La Comisión Federal de Telecomunicaciones reportó durante 2004 usuarios de Internet estimados en 14,036,475, de los cuales 5,521,128 poseen equipos de cómputo en sus hogares y 8,515,347 utilizan Internet fuera de ellos, aunque de éstos 2,634,812 también cuentan con computadoras en el hogar.

XIV. En su informe de labores correspondiente al periodo de 2004 la Secretaría de Seguridad Pública informa sobre las actividades de la Policía Cibernética, en las que reporta durante el año: 101 comunidades en Internet dedicadas a promover la comisión de delitos cibernéticos, 300 páginas dedicadas a promover la prostitución infantil, de las cuales 116 eran mexicanas, y 21 pederastas detenidos.

XV. De igual forma la Procuraduría General de la República informó sus resultados. Durante 2004 en lo concerniente a los delitos de propiedad intelectual, industrial y de derechos de autor, arrojaron 42,600 unidades en software, 8,693,315 fonogramas, 78,570 videojuegos y 1,775,596 videogramas, además de dismantelar 66 laboratorios dedicados a estos ilícitos.

Con base en los antecedentes antes mencionados expongo a este H. Congreso las siguientes:

### **Consideraciones**

I. La necesidad de contar con una legislación eficaz para combatir los delitos cibernéticos es fundamental para la prevenir este tipo de ilícitos, la convergencia internacional en esta materia no deja dudas sobre la preocupación que existe, cada vez más creciente, de que la comisión de esta clase de delitos, constituye un obstáculo difícil de superar en virtud de sus alcances y modalidades en relación al tiempo y a los sujetos que intervienen en ellos.

II. Los sistemas y equipos informáticos se han convertido en una herramienta delictuosa y con ello surge la interrogante que señala hasta donde regular el uso, goce o disposición de ellos y cuando se rebasa la línea de privacidad que las personas poseen. Es en este sentido que esta iniciativa pretende adecuar con precisión cada una de las conductas que demuestran el uso o disposición incorrectos de equipos o sistemas informáticos además, en algunos casos, representan un riesgo para el bienestar común.

III. Las reformas elaboradas al Código Penal, Código de Procedimientos Penales y Código de Comercio que involucran el uso de sistemas y equipos de informática integran legislaciones modelo de organismos internacionales, necesarias para estar a la vanguardia en la regulación de actos jurídicos que incorporan estas

tecnologías y de formas novedosas para hacer negocios gracias a la información que fluye a través de sistemas y equipos informáticos incluyendo sus redes. Son estas las que hacen más complejo el escenario de un delito pues la velocidad de transmisión de datos y la multiplicidad de sujetos que intervienen en el curso de la información dan por resultado una persecución con obstáculos, y más allá de eso, contra reloj.

IV. Desde los organismos internacionales la atención hacia los delitos cibernéticos ha ido en incremento, pues la vulnerabilidad de los sistemas electrónicos y digitales de todos los países alrededor del mundo se han visto afectados desde los niveles gubernamentales y financiero hasta la comunicación personal a través de un teléfono celular. La OEA respondió a esta preocupación con la creación del grupo de expertos por mandato de la Cuarta Reunión de Ministros de Justicia o Procuradores Generales de las Américas en 2002, se consideró la elaboración de los instrumentos jurídicos interamericanos pertinentes y de legislación modelo con el fin de fortalecer la cooperación hemisférica en el combate contra el delito cibernético considerando normas relativas a la privacidad, la protección de la información, los aspectos procesales y la prevención del delito.

V. Las autoridades policiales y de persecución deberán contar en el futuro con los recursos técnicos y humanos para la persecución de estos delitos. En México, la Policía Cibernética perteneciente a la Policía Federal Preventiva es de los primeros cuerpos especializados en Latinoamérica, sólo Brasil y Chile cuentan con un cuerpo policial de este tipo. A lo largo de esta administración ha demostrado su efectividad en el combate a estos delitos y coadyuvando con diversas autoridades en la solución de crímenes que involucran estas tecnologías.

VI. Las estadísticas de la Procuraduría General de la República y la Policía Federal Preventiva sobre delitos que involucran sistemas y equipos informáticos señalan un aumento progresivo de los delitos que afectan a industrias, negocios y consumidores por igual. La disminución de crímenes de este tipo se logra contando con una legislación adecuada y de vanguardia que contemple mecanismos de cooperación entre autoridades locales, estatales, federales e internacionales, tal y como pretende la presente propuesta.

VII. El esfuerzo que hacen las autoridades no es suficiente en ocasiones para combatir los delitos cibernéticos, el trabajo conjunto de cada uno de los sujetos involucrados en este tipo de ilícitos es fundamental para crear una cultura básica de la prevención. El Grupo DC México, involucra a los sectores afectados, convirtiéndose en un grupo de trabajo que evalúa y propone soluciones en el combate a los delitos cibernéticos; en esta ocasión colaboró con esta H. Cámara de Diputados en la elaboración de una propuesta que entregó a la Comisión de Comunicaciones, la cual es base de la presente iniciativa y que se adjunta al respecto.

VIII. Dentro de los compromisos adquiridos al finalizar el Foro sobre Delitos Cibernéticos, estuvo el de impulsar la incorporación de México al Convenio del Consejo de Europa sobre Ciberdelitos, lo cual se cumplió y cuya respuesta de parte de la Secretaría de Relaciones Exteriores fue la siguiente:

"La Convención del Consejo de Europa es un instrumento amplio que contiene disposiciones especializadas para combatir el delito cibernético. La legislación mexicana no contempla muchas de esas figuras. Adicionalmente, serán necesarios recursos para poder instrumentarla de manera específica. En caso que la Cámara de Diputados decida adoptar el Punto de Acuerdo, debería comprometerse, en el mismo documento, a aprobar la legislación que sería necesaria para instrumentarla y a proveer a las autoridades competentes de las partidas presupuestales necesarias con el mismo fin. Conviene recordar que la propia Convención establece un mecanismo de consulta cuyos costos serían sufragados por sus Partes? Asimismo, hago de su conocimiento que se están llevando a cabo las consultas pertinentes para definir la conveniencia de que nuestro país se adhiera a esa Convención y, una vez que haya tomado una decisión sobre el particular, ésta le será comunicada con la debida celeridad"

Esta respuesta justifica el presente instrumento en virtud de que se integran los criterios señalados en la parte sustantiva de la Convención, con el fin de homologar criterios para describir las conductas de los tipos penales. En el aspecto procesal se incluyen algunas en virtud de las características de nuestro sistema jurídico.

IX. Del mismo modo la Cámara de Senadores aprobó un dictamen de la Comisión de Comunicaciones y Transportes, demostrando su preocupación a este respecto y en la cual señala ciertas directrices sobre las cuales

se tiene que legislar y del mismo modo fueron tomados en cuenta en esta iniciativa tal y como lo señalan los resolutivos de dicho dictamen descritos a continuación por oficio recibido en este recinto:

*"Me permito hacer de su conocimiento que en sesión ordinaria celebrada en esta fecha, se aprobó dictamen de la Comisión de Comunicaciones y Transportes, con el siguiente Punto de Acuerdo:*

*"Primero.- Se exhorta a las Legislaturas Locales de las Entidades Federativas, a que legislen en temas que sean de su competencia y/o concurrencia, a efecto de que incorporen disposiciones jurídicas similares a las contenidas en el Código Penal Federal, en el Libro Segundo, Título Noveno denominado, Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática.*

*Segundo.- Se reconoce a la Comisión de Comunicaciones de la Cámara de Diputados, quien se encuentra trabajando en una Iniciativa de Ley, a que continúe con la conformación de la misma, para que se pueda contar con una legislación que tipifique las conductas delictivas que ponen en riesgo la seguridad de los consumidores; de los sitios de Internet; del comercio electrónico en general; y de los titulares de derechos.*

**Tercero.- Se exhorta al Ejecutivo federal, para que considere la posibilidad y beneficios de que México se adhiera a los Tratados Internacionales que existen sobre la materia, a efecto de poder prevenir actos delictivos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional".**

Los resolutivos señalan sugerencias para que se legisle en esta materia además de reconocer la iniciativa que a este respecto elabora la Comisión de Comunicaciones. Ello se puede solventar con esta y las demás iniciativas presentadas por integrantes de la Comisión en el período ordinario pasado ya que tienen como base la propuesta de DC México.

X. Las propuestas legislativas concretas y las prioridades que, según los distintos miembros del Subgrupo Jurídico de DC México, debían legislarse prioritariamente son varias:

a) Microsoft

Se debe procurar que la iniciativa que se redacte se ajuste a los términos o conceptos jurídicos existentes, sin variar su connotación ya establecida por otras leyes, tal como puede ocurrir, por ejemplo, respecto de términos jurídicos como "daño", "mensaje de datos", o la determinación de conductas con "dolo" o "culpa".

Por otra parte, se debe sustituir el término "computadora" por el de "sistemas o equipos informáticos", e incluso ampliarlo hasta el Internet.

Adicionalmente, proporciona definiciones distintas a las de la iniciativa de la LVIII legislatura en materia de pornografía infantil y datos personales, acotando los límites respecto acerca de las conductas ilícitas en esta última materia.

Para el tema de la penalización del *spam*, se sugiere la revisión de la *can-spam* de los Estados Unidos de América.

Señala Microsoft su preocupación respecto de otros temas como la protección de privacidad y datos personales, que involucran cuestiones de "robo de identidad" (ID Theft), que ya son motivo de discusión en otros foros del ámbito legislativo y financiero, y que implicarán la promulgación de nuevas leyes y reformas o adiciones en leyes existentes, cuya circunstancia tendrá necesariamente un impacto sobre la regulación que se efectúe en materia de delitos cibernéticos.

Se deberá atender y definir nuevos conceptos y sujetos de regulación, así como delimitar los casos y rangos de responsabilidad de los proveedores de servicio de Internet y/u otros agentes intermediarios en el almacenamiento o transmisión de información que potencialmente pueda ser delictiva per se o por su eventual

uso para la comisión de delitos, bajo el criterio de control; desde el punto de vista procesal, restringir la responsabilidad de dichos proveedores o agentes y determinar los casos y condiciones en los cuales queden obligados a proporcionar información, en rangos razonables y operativos.

Sugiere la inclusión del siguiente texto: "Las conductas previstas en el presente [título, artículo] únicamente podrán ser atribuidas a un proveedor o sus representantes [o Proveedor de Servicio de Internet, o ISP según se defina] en la medida en que el servidor o cualquier otro medio de almacenamiento o transmisión de que se trate, a través de los cuales se actualicen aquéllas, estén bajo su control o se lleven a cabo de forma personal y directa por dicho proveedor o sus representantes".

Determinar con claridad los delitos que requieren calidad objetiva, subjetiva o ánimo en particular (por ejemplo, casos en los que se requiera el ánimo de lucro o de comisión subsecuente de otro delito).

Circunscribirse a delitos del orden federal o procurar definición de los del orden común en los ordenamientos respectivos.

## **b) Mercado libre**

Agregar una definición sobre Proveedor de Servicios que establezca que se trata de aquella entidad pública o privada que presta un servicio por medio de un sistema informático a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

Se sugiere el siguiente texto en materia de Fraude Informático o cometido por medio de un sistema informático:

*"el que con ánimo de lucro y valiéndose de cualquier ardid o engaño, perjudicare patrimonialmente a otro mediante la utilización de un sistema informático, sea modificando datos, sea introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee los procedimientos de seguridad del sistema, se le impondrá la pena de ...".*

Mercado Libre sugiere limitación de responsabilidad de los prestadores de servicios de Internet bajo la incorporación del procedimiento de "Notice & Take Down" en los siguientes términos:

El Proveedor de Servicios no será responsable por el contenido de terceros por él almacenados, si:

1. Desconoce que el contenido de la información es ilícito;
2. Retira o bloquea el acceso a la información inmediatamente de tomar conocimiento de su carácter ilícito.

### **- Mera transmisión**

Responsabilidad de los Prestadores de Servicios: El Prestador de Servicios de transmisión de datos no será responsable por el contenido de las comunicaciones que transmite si no es él mismo el originante; ni es él mismo quien seleccione al destinatario; ni es él mismo quien selecciona o modifica los datos transmitidos.

- Obligaciones. La exclusión de responsabilidad prevista anteriormente, no afecta las obligaciones emergentes de la aplicación de normativas regulatorias específicas ni las obligaciones contractuales asumidas en su caso por parte de proveedores de servicios intermediarios.

-Memoria transitoria. El Proveedor de Servicios no será responsable por el almacenamiento automático, provisional y temporal de datos suministrados por sus clientes o usuarios, si:

1. No modifica la información;

2. Actúa con prontitud para retirar la información que haya almacenado o bloquea su acceso, en cuanto tenga conocimiento efectivo a raíz de una notificación del titular del derecho de propiedad intelectual o que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella.

- Inexistencia de obligación general de supervisión.

Los Proveedores de Servicios no están obligados a supervisar los datos que transmiten y almacenan; ni están obligados a realizar búsquedas activas de hechos o circunstancias que, en el ámbito de los servicios que prestan, indiquen la existencia de actividades ilícitas.

**c) Asociación Mexicana de Internet (AMIPCI)**

Se sugiere incorporar dentro de los delitos en los que los medios electrónicos sirven como medios comisivos el término de mensaje de datos y sistemas informáticos, a efecto de lograr la equivalencia funcional.

**d) Alestra**

Presenta una propuesta de punto de acuerdo a efecto de que la H. Cámara de Diputados solicite del Senado se sirva revisar el texto de la Convención de Cibercriminos del Consejo Europeo para, en su caso, que el gobierno federal suscriba el citado instrumento.

Deben evitarse los requerimientos extra-legales de información y acciones que comprometen la operación y desarrollo de importantes elementos y actores que hacen posible la industria de las Tecnologías de Información y Comunicaciones en nuestro país y todos sus beneficios derivados a la sociedad.

**e) Instituto Tecnológico Autónomo de México (ITAM)**

Buscar la unidad en la legislación sustantiva y adjetiva a nivel estatal, federal e internacional.

Proteger los datos personales y las redes de infraestructura crítica.

Adoptar la Convención de Cibercriminos del Consejo Europeo suscrita por los estados del Viejo Continente, Japón, Sudáfrica, EE.UU.A., Canadá, (miembros del TLCAN), toda vez que establece un catálogo mínimo de delitos que por estar en la Convención se consideran extraditables, así como las medidas procesales para la obtención de evidencia por parte de las autoridades conducentes y una efectiva Cooperación Internacional.

Considerar el documento denominado Creación de una Sociedad de la Información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos.

**f) Centro de Inteligencia para la Seguridad Nacional (CISEN)**

Es preciso revisar los elementos normativos para llevar a cabo investigaciones en torno a terrorismo, atentados contra la infraestructura estratégica gubernamental y ataques a entidades estratégicas de la economía nacional

No existe ninguna ley que obligue a ISP a entregar la información respecto de una investigación sin hay una orden judicial. Cada empresa procede de manera autónoma ante las solicitudes para entregar evidencias electrónicas y los tiempos y trámites son excesivos para la entrega de la información.

Falta de reconocimiento y validez jurídica de la evidencia digital en México.

Falta de legislación y procedimientos en materia de manejo de evidencia electrónica.

Se requiere de jueces y peritos especializados en materia de delitos informáticos.

**g) Procuraduría General de la República (PGR)**

No se deben tipificar conductas ilícitas independientes a los tipos penales clásicos como el fraude, cuando las mismas sean contenidas a través del uso de computadoras, ya que ello implica elevar a rango de delito el uso de un medio comisivo determinado. En todo caso, se considera apropiado revisar los tipos penales de mayor incidencia que son cometidos a través de sistemas de cómputo, en aras de concluir si efectivamente es necesario incorporar en las descripciones penales correspondientes el medio comisivo en comento.

Determinar en forma general el bien jurídico o tutelar, a fin de establecer claramente si se sanciona el acto o al autor, que en opinión propia debiera ser en relación al acto mismo y no al autor.

Se considera necesario tipificar las conductas ilícitas que atentan contra los sistemas de cómputo que no estén previstas en la legislación federal vigente tales como la interceptación ilícita de datos, la denegación del sistema o la producción o venta de dispositivos para la comisión de delitos cibernéticos.

Se considera oportuno que la legislación prevea la obligación de los proveedores de Internet para resguardar la información de sus clientes por un determinado periodo de tiempo.

En materia procesal, no obstante que el Ministerio Público tiene la facultad de solicitar a los proveedores de Internet la información que tengan respecto de sus usuarios, siempre y cuando, ello no implique intervención de comunicaciones privadas, de conformidad con el artículo 180 del Código Federal de Procedimientos Penales, se debe explorar la posibilidad de prever expresamente la facultad de la autoridad ministerial en aras de evitar controversias judiciales.

Se considera oportuno que la legislación prevea los mecanismos legales necesarios para superar los obstáculos que implica el hecho de que varios proveedores de Internet se encuentren constituidos en el extranjero.

#### **h) Comisión Federal de Telecomunicaciones (Cofetel)**

Incluir en la definición de "daño" el concepto de sistemas o equipos informáticos en lugar de computadoras y homologarlo en la medida posible con la definición de daño dado en el artículo 2108 del Código Civil Federal. No obstante lo anterior, sería conveniente considerar la eliminación de este rubro toda vez que la destrucción, descompostura, deterioro o menoscabo causado a computadoras representa un daño más bajo en el contexto de responsabilidad civil por daño a bienes ajenos, que un delito informático en sí mismo.

En la definición de datos personales, sería conveniente sustituir los calificativos de "identificada o identificable" por "que la identifique o haga identificable" e, igualmente clarificar a que se refiere la disposición cuando establece "entre otra", de qué otro tipo sería esta?

En materia de pornografía infantil sería conveniente considerar aún aquellas representaciones que se realice sobre personas o menores aún aquellas que no existan en la realidad.

Respecto del Código Penal Federal existe una inconsistencia en el artículo 211 bis 1 al señalar que sólo cometen el delito de acceso ilícito a sistemas y equipos informáticos cuando las acciones descritas por la disposición legal en comento son aplicadas a equipos o sistemas informáticos que se encuentren protegidos (esto implica que los no protegidos sí pueden ser violentados?)

En el artículo 368 de la iniciativa se estableció que se equiparan al robo?III. La copia?o el aprovechamiento o utilización de dichos documentos, datos o archivos sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos, lo que da pie a una serie de posibilidades tales como que, exista derecho pero no consentimiento, o que no exista el derecho pero si el consentimiento, siendo únicamente bajo el contexto de una presentación conjunta de ambos que la acción encuadre con el tipo penal establecido; asimismo en su caso será necesario definir el concepto de "disponer".

En relación al artículo 211 bis 2 de la iniciativa, resulta inadecuado establecer como atenuante del delito el no causar un daño, ya que la conducta descrita lo establece como elemento esencial del tipo penal ahí establecido y, siendo el derecho penal de aplicación estricta en caso de no darse el daño no se estaría ante el tipo penal descrito.

Se debe determinar claramente en qué tipos penales planteados es posible establecer el grado de tentativa; ya que no en todos es aplicable y posible.

Será necesario determinar cómo se medirá el daño por ejemplo, en el caso de pérdida o comercialización de información o datos personales.

Establecer medios de cooperación internacional e interestatal para no sobrepasar los límites de la jurisdicción.

i) Secretaría de Trabajo y Previsión Social (STPS)

Organización Internacional del Trabajo (OIT)

Instituto Nacional de Ciencias Penales (Inacipe)

En el Código Penal Federal se sanciona con la pérdida del beneficio de la libertad preparatoria a quien se dedique a la corrupción, pornografía, turismo y trata de menores, también castiga a quien corrompa a los menores, los induzca a la pornografía infantil, o a quien grave o videograve, administre o financie, posea o distribuya por medios electrónicos pornografía infantil.

De igual manera se sanciona al que promueva por cualquier medio el turismo sexual con menores.

Asimismo, el Código Federal de Procedimientos Penales sanciona considera delito grave la corrupción, pornografía y turismo sexual de menores.

La Ley contra la Delincuencia Organizada establece que la corrupción, pornografía y turismo sexual de menores entra en el rubro de actividades de la delincuencia organizada.

Finalmente la Ley para la Protección de los derechos de niñas, niños y adolescentes fomenta las actividades de prevención en contra de los ilícitos citados con anterioridad.

XI. Las modificaciones que se pretenden se justifican en el orden que a continuación se describen:

## **1. Código Penal Federal**

Las adiciones que se proponen son:

**Las de un Título Vigésimo Séptimo denominado Delitos Cibernéticos** pues se consideran delitos especiales por su propia naturaleza, siguiendo así el mismo criterio de los Delitos Ambientales consignados en el Título Vigésimo Quinto y los Delitos en materia de Derechos de Autor en el Título Vigésimo Sexto. El capitulado obedece a un criterio de redacción general del libro cuyo catálogo de delitos asigna unitariamente un capítulo por delito. Así el concepto o delito es señalado como parte del título del Capítulo y la descripción del tipo penal se encuentra en el texto del artículo. Además son 9 artículos cuya inclusión dentro de la seriación numérica del Código utilizando latinismos numéricos, corrompería la integridad y en ocasiones la congruencia del cuerpo legal.

**Las de incluir un Capítulo IV al Título Octavo con el nombre de Disposiciones comunes para este Título**, en virtud de incluir en él, definiciones de términos técnicos o confusos, utilizados particularmente en la redacción del articulado de los Capítulos II y III, con el fin de hacerlos más comprensibles para definir el tipo penal.

**Del Título Vigésimo Segundo, la fracción tercera del artículo 368 del Capítulo Primero.** Con esta adición se pretende incluir el robo de información digital, virtual o de naturaleza electrónica en virtud de que existen delitos de otra índole en los que se comete robo de identidad o de datos personales para la comisión del mismo. Particularmente el Código de Comercio y el Código Civil ya contemplan la figura de la firma electrónica cuya falsificación o abuso en la disposición del mismo no sería tutelado.

La reforma que se proponen al Libro Primero es la siguiente:

**El inciso c) del artículo 85 del Capítulo Tercero del Título Cuarto.** Relativo a las causales por las cuales se niega la libertad preparatoria, cuyos cambios en los conceptos de las conductas ilícitas aclaran su significado detallando el concepto y evitan términos discriminatorios u ofensivos para personas con capacidades distintas. Se incluyen los delitos de pornografía infantil y lenocinio infantil en un sentido de congruencia con la afectación en el desarrollo humano y sus consecuencias que sufren los menores al paso del tiempo.

Las correspondientes al Libro Segundo y su catálogo de delitos a continuación se describen.

**El artículo 139 del Capítulo Sexto del Título Segundo. Terrorismo.** Consideramos que es necesaria esta reforma pues ante la vulnerabilidad de los avances tecnológicos utilizados en la prestación de servicios básicos públicos y privados, existe el riesgo latente de sufrir un ataque masivo de singulares características propias de los sistemas y equipos informáticos pero que sus consecuencias serían serias y de gravedad no solamente doméstico sino internacional. Carecemos de una figura homologada a lo que internacionalmente se denomina ciberterrorismo. Sobre todo que comprenda todas las características del tipo penal que actualmente describe al terrorismo, por ello consideramos agregar a su redacción, como medio comisivo, el ataque masivo a estas herramientas.

**Del Título Octavo se reforma su denominación de "Delitos contra la moral pública y las buenas costumbres" a "Delitos que lesionan el desarrollo humano".** Conceptos como moral pública y buenas costumbres son ideas o conceptos que a través del tiempo han sido utilizados para calificar determinadas conductas como socialmente inapropiadas, resultado de convencionalismos sociales. Dice García Maynez " ... *Generalmente, los convencionalismos son exigencias tácitas de la vida colectiva, es decir, carecen de una formulación expresa y absolutamente clara; pero nada impide admitir la posibilidad de que se les formule e inclusive se les codifique. Una prueba de ello la encontramos en los manuales de urbanidad y los códigos de honor.*"<sup>1</sup> El debate acerca de la codificación de los convencionalismos proviene desde la Teoría del Derecho, y sus distintas escuelas. Así, ha correspondido a los tribunales judiciales y a la Suprema Corte hacer interpretaciones jurídicas acerca de los valores; ello provoca que la norma jurídica, imperfecta de origen, carezca de claridad y precisión, razón por la cual se sugiere en este proyecto la sustitución de la denominación del Título. Si bien, el título es algo representativo también es necesaria su concordancia con las normas jurídicas que agrupa. De esta forma se plantea un título más congruente y aplicable a los artículos contenidos con base en un concepto clínico y humanista.

**Del mismo Título, la denominación de su Capítulo Segundo, sus artículos 201, 202, 203, 204, 205, 206, 207, 208 que se integra al Capítulo Cuarto; con ello se derogan los artículos 201 bis, 201 bis 1, 201 bis 2, 201 bis 3.** Con respecto a estos artículos se ordena y precisa las conductas y las sanciones correspondientes. Se comienza proponiendo un cambio al título del Capítulo para adecuarlo al cuerpo normativo y por las mismas razones del Considerando anterior. Se propone dividir cada conducta o sanción en fracciones para una mejor comprensión. Algunos párrafos se rectifican en otros artículos relativos y se amplían los conceptos, señalando conducta por conducta el tipo penal específico. El margen de diferencia entre la mínima y máxima pena aplicable es amplio para que el juez pueda aplicarla considerando el daño causado, las consecuencias del delito y las secuelas que pudiera sufrir eventualmente la víctima. Para ello se incluye también un artículo que contempla agravantes. También se define mejor el delito de Trata de Personas y el de Lenocinio y se incluye un artículo que define los delitos y otros conceptos técnicos complejos para acreditar con mayor eficacia el cuerpo del delito o la evidencia.

**Del Título Noveno se elimina de su denominación la frase "Acceso ilícito a sistemas y equipos de informática" para quedar únicamente como "Revelación de Secretos".** En virtud de que hay una incongruencia con el título original del Código que señalaba originalmente "Revelación de Secretos" y para la reforma de 1999 al Código Penal en comento, se incluye la frase Acceso Ilícito a Sistemas y Equipos de Informática exhibiendo una deficiente técnica jurídica, toda vez que se desvirtúa la composición del Título añadiendo no sólo un elemento objetivo que en absoluto tiene que ver con la materia del titular, sino que añade artículos que regulan otro objeto y materia distintos. Ello es respaldado por la numeración deficiente del articulado que lejos de respetar la secuencia lógica jurídica del Código, resalta la deficiente reforma elaborada, más aún por la longitud del capítulo equívocamente añadido. De tal modo que la propuesta que se expuso en el

primer considerando de esta iniciativa, consideramos, es la correcta al contemplar un capítulo distinto, de modo que posea cierta flexibilidad para posteriores reformas debido a la naturaleza de la materia y cuya longitud no sea un inconveniente dentro de la actual secuencia numérica que posee la ley.

**Del Título Vigésimo Sexto los artículos 424 bis y 426.** Que se refieren a los Delitos en Materia de Derechos de Autor se elimina la fracción segunda del artículo 424 bis en virtud de que se solventa con el artículo 431 propuesto como Acceso no autorizado a sistemas y equipos de informática pues la conducta que contempla la fracción II se tipifica de mejor forma en el numeral mencionado. En lo que respecta al 426 su relación es muy estrecha con un delito cibernético en comento, si bien se corrigió su redacción en lo concerniente a señalar detalles que no contempla aquél.

## **2. Código Federal de Procedimientos Penales**

Las reformas que se proponen son:

**El artículo 175** para la conformación del cuerpo del delito y la probable responsabilidad del inculpado hay que señalar ciertas características comunes a todos, como es el uso de un equipo o sistema informático, las circunstancias en las que se utiliza y los conocimientos que tenga el indiciado al respecto, la dificultad de probar este tipo de delitos, hace necesario el dar reconocimiento y validez jurídica a la evidencia digital, a la información contenida y transmitida a través de equipos y sistemas informáticos. También los conocimientos del indiciado en esta materia influye en la complejidad del delito en particular cuando es uno solo el autor, sin embargo, la dificultad se presenta al momento de acreditar el delito. Para que esta iniciativa se complete es necesario dar el suficiente valor probatorio a este tipo de elementos, evidentemente para no provocar un desajuste, esto solo se circunscribe a los delitos cibernéticos, de modo tal, que no será reconocido como medio de prueba para algún otro a menos que haya "*información*" involucrada en el delito que textualmente describa el tipo penal.

**El artículo 194** por su parte nos describe cuales son los delitos clasificados como graves y en este aspecto se propone incluir la corrupción de menores, la pornografía y lenocinio infantiles por su naturaleza y las consecuencias que sufren los menores víctimas de estos delitos y que se manifiestan al crecer como seres humanos.

**El artículo 285** excluye a la evidencia digital y a la *información* de ser consideradas como meros indicios en virtud de la excepción señalada para el artículo 175 que expresamente señala "... para el caso de los delitos cibernéticos...." y ello también con la finalidad de limitarlos o circunscribirnos exclusivamente a comprobar esta clase de delitos por la naturaleza de los mismos.

## **3. Ley Federal Contra la Delincuencia Organizada**

**La fracción V del artículo 2** contempla como delincuencia organizada el tráfico de menores. Consideramos dentro de este contexto, agregar los delitos de Corrupción de Menores, Pornografía infantil y Lenocinio Infantil. Ello porque para su ejecución o para que se realice el delito descrito en la norma, en muchas ocasiones convergen 3 o más individuos, sobretodo cuando se busca un lucro a través de esta actividad.

**Los artículos 20, 22 y 23**, la propuesta solo es de agregar el concepto de *dispositivos, ópticos electrónicos o magnéticos*, en virtud de que la información, incluyendo el audio y video, se pueden almacenar y transportar en este tipo de dispositivos de distinta índole, y que actualmente son de mayor utilidad para llevar a cabo todas las investigaciones de forma rápida y eficiente, evitando así limitarlos únicamente al uso de dispositivos magnéticos.

## **4. Ley de la Policía Federal Preventiva**

Dentro del inciso a) de la fracción III dentro del artículo 4 se señalan las atribuciones de la Policía Federal Preventiva garantizar, mantener y restablecer el orden y la paz públicos, salvaguardar la integridad de las personas, así como prevenir la comisión de delitos. En este sentido se decidió incluir en este inciso *el tráfico de información a través de Internet* es necesario formalizar este aspecto, porque aunque su Policía Cibernética

atiende ya la vigilancia en este aspecto, también es cierto que no está contemplado expresamente dentro de sus atribuciones. El concepto Internet es ya universalmente aceptado e incluido en otras legislaciones internacionales, adoptado también dentro del Diccionario de la Real Academia de la Lengua Española y reconocido universalmente por ello la conveniencia de incluirlo en la redacción del texto legal.

## **5. Transitorios**

El artículo Segundo Transitorio del presente instrumento pretende formalizar la Unidad de Policía Cibernética dentro de la Estructura Orgánica de PFP, si bien, si existe en la estructura orgánica como Departamento de Análisis de Delitos Cibernéticos, dependiente de la Dirección General de Tráfico y Contrabando, que por cierto poco tiene de relación, también es necesario que para una mayor eficacia y organización de recursos financieros humanos y materiales sea concebida como un cuerpo especializado y contemplado orgánicamente.

El Tercero Transitorio se redacta con el fin de hacer comprensibles los delitos cibernéticos a las autoridades administrativas y judiciales en virtud del lenguaje técnico que se utiliza para su valorización. Para ello es necesaria la capacitación en este tipo de temas, por ello se le consultó a la Policía Cibernética si accedía a ser responsable de esta tarea a lo cual accedió puntualizando que no solamente serían las autoridades administrativas y judiciales, sino también en la creación de las policías cibernéticas estatales, estarían dispuestos a coadyuvar con el fin de uniformizar criterios de aplicación de la ley y persecución.

El artículo Cuarto Transitorio, formaliza la creación de DC México como un grupo interinstitucional de consultoría y asesoría de combate a delitos cibernéticos, se contempla también que ejerza estas funciones para combatir el correo electrónico, tipo *spam* (mensaje de datos comercial no solicitado), pues causa un perjuicio social, así como otras conductas que causen un perjuicio social a través de la utilización de Internet o de redes públicas o privadas de telecomunicaciones.

El artículo Quinto Transitorio se redacta atendiendo a la persecución de los delitos cibernéticos, cuya reacción ante estos ilícitos tiene que ser pronta y expedita, debido a su naturaleza y al vertiginoso tráfico de información a través de redes e Internet. Para ello la colaboración entre autoridades estatales federales e inclusive internacionales tiene, por lo menos, ser igual de pronta para afrontar con eficacia estos delitos. Los distintos convenios de colaboración pueden solventar esto.

Por las motivaciones expuestas anteriormente, someto a consideración de esta H. Asamblea la siguiente iniciativa con proyecto de decreto:

### **Artículo Primero.- Se modifican del Código Penal Federal las siguientes disposiciones:**

**I. Se adicionan al Libro Segundo: el Título Vigésimo Séptimo denominado Delitos Cibernéticos constante en ocho artículos, con numerales desde el artículo 430 al 438 y divididos en cuatro capítulos; el Capítulo Cuarto del Título Octavo; el artículo 251 bis dentro del Capítulo Octavo del Título Decimotercero; y la fracción tercera al artículo 282 del Capítulo Primero del Título Decimotercero. Del Título Vigésimo Segundo, una fracción tercera del artículo 368 del Capítulo Primero**

**II. Se reforma del Libro Primero: el inciso c) del artículo 85 del Capítulo Tercero del Título Cuarto. Del Libro Segundo se reforman: el artículo 139 del Capítulo Sexto del Título Segundo; del Título Octavo se reforma su denominación de "Delitos contra la moral pública y las buenas costumbres" a "Delitos que lesionan el desarrollo humano", de su Capítulo Segundo su título y los artículos 201, 202, 203, 204, 205, 206, 207, 208 que se integra al Capítulo Cuarto, y de éste último el 209; del Título Noveno se elimina de su denominación la oración "Acceso ilícito a sistemas y equipos de informática" para quedar únicamente como "Revelación de Secretos"; del Título Vigésimo Segundo el artículo 386 del Capítulo Tercero; y del Título Vigésimo Sexto los artículos 424 bis y 426.**

**III. Se derogan del Libro Segundo: los artículos 201 bis, 201 bis 1, 201 bis 2, 201 bis 3, del Capítulo Segundo en el Título Octavo.**

## **IV. Se abroga el Capítulo Segundo del Título Noveno**

**Lo anterior para quedar como sigue:**

### **Código Penal Federal**

#### **Libro Primero**

#### **Título Cuarto**

#### **Capítulo III**

#### **Ejecución de Sentencias.**

Artículo 85.- No se concederá la libertad preparatoria.....

I. ....

a) ...

b) ...

c) Corrupción de menores o de quienes son incapaces para comprender el significado del hecho, pornografía infantil, lenocinio infantil; previstos en los artículos 201, 202 y 204, respectivamente.

d) a j)

II. ...

### **Libro Segundo**

#### **Título Segundo.- Delitos contra la Seguridad de la Nación.**

#### **Capítulo VI.- Terrorismo**

Artículo 139.- Se impondrá pena de prisión de dos a cuarenta años y multa hasta de cincuenta mil pesos, sin perjuicio de las penas que correspondan por los delitos que resulten, al que utilizando: explosivos, sustancias tóxicas, armas de fuego, la comisión de incendios o inundaciones, *ataque masivo a sistemas o equipos informáticos, cualquier otra tecnología, u otro medio violento*; realice actos en contra de las personas, cosas o servicios al público, que produzcan alarma, temor terror en la población o en un grupo o sector de ella, para perturbar la paz pública, o tratar de menoscabar la autoridad del Estado, o presionar a la autoridad para que tome una determinación

#### **Título Octavo.- Delitos que lesionan el desarrollo humano.**

#### **Capítulo II**

#### **Corrupción, Pornografía, Lenocinio en Menores y Personas con Capacidades Distintas**

Artículo 201.- Comete el delito de corrupción de menores, o de personas que no tengan la capacidad para comprender el significado del hecho, quien incite, induzca, facilite, provoque o procure en menor de edad o persona con capacidades distintas, las conductas que se sancionan a continuación:

I. Realizar actos de exhibicionismo corporal. Se castigará con cinco a nueve años de prisión, y de quinientos a mil doscientos días de multa;

II. El alcoholismo, o el consumo de estupefacientes, psicotrópicos, o sustancias tóxicas, de manera ilegal. Se sancionará con cinco a diez años de prisión y multa de seiscientos a dos mil días de multa, más el costo de la rehabilitación del menor;

III. El pandillerismo o la asociación delictuosa. Se sancionará con prisión de siete a doce años y multa de doscientos a quinientos días, independientemente de las que puedan corresponder a estas conductas sancionadas por este código;

IV. La comisión de algún delito. La sanción será aumentada hasta en una mitad de la pena correspondiente al delito cometido.

V. La práctica de la mendicidad. Se impondrá de 1 a 5 años de prisión y de doscientos cincuenta a 800 días de multa, y

VI. Presten sus servicios en establecimientos, cuya autorización de funcionamiento, prohíba su contratación o ingreso; no obstante si es regular o irregular. Incurrirán en las mismas penas los padres o tutores que permitan lo anterior a sus hijos o menores que estén bajo su guarda o custodia.

Si derivado de las conductas anteriores el menor o la persona adquiriese un hábito o una dependencia de cualquier tipo se deberán aumentar las sanciones previstas hasta en una tercera parte.

No se entenderá por corrupción de menores los programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, educación sobre función reproductiva, la prevención de enfermedades de transmisión sexual y el embarazo de adolescentes, siempre que estén aprobados por la autoridad competente.

Artículo 202.- Comete el delito de pornografía de menores, o de personas que no tengan la capacidad para comprender el significado del hecho, quien, con el fin de exhibir, publicar, distribuir, o comercializar, imágenes, secuencias de video o sonidos con contenido sexual, a través de cualquier medio de comunicación o de sistemas y equipos informáticos, realice las actividades que a continuación se describen:

I. Incite, induzcan, faciliten, provoquen, procuren u obliguen a menores de edad o personas que no tengan la capacidad para comprender el significado del hecho, a realizar actos de exhibicionismo corporal, o pornografía;

II. Participe en la elaboración de imágenes, fotografías, filmaciones o grabaciones, a través de cualquier técnica, sistemas o equipos informáticos u otra tecnología; en los cuales consten actos de exhibicionismo corporal o pornografía, donde participen menores de edad o personas que no tengan la capacidad para comprender el significado del hecho;

III. El que financie o patrocine, promueva, invite, o gestione a personas que realicen las actividades de la fracción I y II, y

IV. El que copie, ofrezca, venda, arriende, publique, distribuya, transmita o posea cualquier dispositivo de almacenamiento óptico, electrónico o magnético, donde consten los elementos señalados por la fracción II.

Artículo 203.- Las sanciones y agravantes respecto al delito de pornografía de menores atenderán de forma particular a la víctima, el daño físico, fisiológico, emocional o moral que pueda padecer con sus consecuencias; y la relación del autor respecto al ofendido conforme al margen siguiente:

I. De 6 a 12 años de prisión y de 400 a 2500 días de multa, si la persona ofendida fuese mayor de 14 y menor de 18;

II. de 10 a 18 años de prisión y de 800 a 4000 días de multa si la víctima fuese mayor de 10 y menor de 14, y

III. De 14 a 25 años de prisión y de 1000 a 6000 días de multa si la persona ofendida fuese menor a 10 años.

También se decomisarán los objetos, instrumentos y demás dispositivos que formen la evidencia del delito, o que se integren como pruebas del mismo, así como la información que resida en sistemas o equipos informáticos propiedad de terceros en cuyo caso se extraerá únicamente la necesaria para perseguir el delito respetando sus derechos respectivos.

Artículo 204.- Comete el delito de lenocinio infantil el que cometa alguna de las actividades descritas a continuación y que se sancionarán atendiendo a la magnitud del daño físico, fisiológico, moral o emocional que eventualmente sufran las víctimas, así mismo se sancionará de la siguiente forma:

I. Induzca, promueva, facilite u obligue la prostitución de menores de edad o incapaces, independientemente de recibir una contraprestación por ello; se sancionará con pena de 7 a 15 años de prisión y de 2000 a 6000 días de multa.

II. El que ejerza el comercio carnal sobre menores de edad o incapaces; se aplicará una pena de 7 a 15 años de prisión y de 1000 a 8000 días de multa.

Comete el delito de promoción de prostitución de menores de edad o quienes no tienen capacidad para comprender el significado del hecho, el que promueva, invite, facilite o gestione por cualquier medio el viaje de personas hacia el interior o exterior del territorio nacional con el propósito de practicar actos sexuales o que impliquen corrupción o pornografía con menores de edad o con quienes no tienen capacidad para comprender el significado del hecho.

Artículo 205.- Las sanciones correspondientes a los delitos señalados en el artículo 201, 202 y 204 se aumentarán de conformidad con lo siguiente:

Hasta en una tercera parte, si el delito es cometido por servidores públicos, o por aquél que ejerza autoridad sobre la víctima en virtud de cualquier relación. El servidor público será inhabilitado para desempeñar cualquier cargo público hasta por un tiempo equivalente al de la pena en prisión que corresponda.

Hasta en una mitad, si el delito es cometido por ascendientes sin límite de grado, familiares en línea colateral hasta cuarto grado; tutores o curadores; quienes ejerzan la patria potestad, guarda o custodia sobre el menor; por quien habite con la víctima; por ministro de algún culto religioso; o a través de violencia física o moral.

Los familiares directos o indirectos de la víctima, los que ejerzan la patria potestad sobre su descendencia o sobre la víctima, perderán todos los derechos y beneficios que por ley les correspondan o de los cuales gocen.

Asimismo los responsables de los delitos contemplados en este capítulo quedarán inhabilitados para ser tutores o curadores.

### **Capítulo III. De la Trata de Personas y Lenocinio**

Artículo 206.- Comete el delito de Trata de Personas quien promueva realice o fomente la migración de personas, a través de engaños, o aprovechándose de la situación en la que se encuentran, para ser sometidas al comercio carnal. La sanción será la que corresponda al lenocinio aumentada hasta en una mitad.

Artículo 207.- Comete el delito de lenocinio:

I. Toda persona que habitual o accidentalmente ejerza el comercio carnal, subsista de él u obtenga cualquier contraprestación de él.

II. Al que induzca, promueva, facilite, encubra, o intermedie a favor de alguien y en nombre de una persona para someterla al comercio carnal incluida la prostitución.

III. El que se ostente como responsable, administre o sostenga directa o indirectamente prostíbulos, casas de cita o lugares de concurrencia expresamente dedicados a explotar la prostitución u obtenga cualquier beneficio con sus servicios.

El lenocinio se sancionará con prisión de 6 a 15 años y de 100 a 3000 días de multa, y atenderá a la magnitud del daño físico, fisiológico, moral o emocional que eventualmente sufran las víctimas. Si la víctima es un menor de edad o alguna persona que no tenga capacidad para comprender el hecho, se aumentará la pena hasta en una mitad.

#### **Capítulo IV**

##### **Disposiciones Comunes para este Título**

Artículo 208.- Para los efectos de este Título se entenderá como:

Menor de edad.- La persona menor de dieciocho años cumplidos, al día en que se comente el delito.

Persona que no tiene capacidad para comprender el significado del hecho.- Las personas con capacidades distintas, los mayores de edad disminuidos o perturbados en su inteligencia, aunque tengan intervalos lucidos; y aquellos que padezcan alguna afección originada por: enfermedad o deficiencia persistente de carácter físico, psicológico o sensorial, o la originada por adicción al alcohol, los psicotrópicos, los estupefacientes u otras sustancias tóxicas. Siempre que, debido a la limitación o a la alteración en la inteligencia que esto les provoque, no puedan gobernarse y obligarse por si mismos o manifestar su voluntad por algún medio.

Exhibicionismo Corporal.- Representación fija o en movimiento del cuerpo humano con fines de lascivia sexual real o simulada.

Pornografía.- Representación real o simulada del cuerpo humano a través de cualquier medio visual o auditivo, involucrado explícitamente en un acto sexual o de lascivia respecto al mismo.

No se considerarán como tal las imágenes, fotografías, grabaciones de audio o video contenidas en sistemas o equipos informáticos, o de otra tecnología y que sean programas preventivos, educativos o de cualquier índole que diseñen e impartan las instituciones públicas, privadas o sociales que tengan por objeto la educación sexual, prevención de enfermedades de transmisión sexual, o el embarazo.

Prostitución.- Actividad a la que se dedica quien mantiene relaciones sexuales con otras personas, a cambio de alguna contraprestación.

Comercio carnal.- Aquél que se realiza con personas privadas de su libertad o sometidas, para ser explotadas de cualquier modo, incluyendo sus órganos, tejidos o componentes físicos, independientemente de que se obtenga un lucro o contraprestación de cualquier índole por ello.

Vicio.- Gusto especial por actividades, cuya naturaleza de su objeto, incitan a realizarlas frecuentemente con exceso, que como propiedad o costumbre, tienen algunas personas o es común a una colectividad; y como consecuencia, les provoca trastornos físicos, fisiológicos o mentales.

Artículo 209.- Cuando de la comisión de los delitos a que se refiere el presente Título, resultaren otros delitos se estará a las reglas del concurso.

#### **Título Noveno.- Revelación de Secretos**

#### **Título Decimotercero.- Falsedad**

#### **Capítulo VIII**

##### **Disposiciones Comunes a los Capítulos Precedentes.**

Artículo 251 bis.- Para los efectos de este título, también se entenderá por documento a los mensajes de datos que consten o sean susceptibles de reproducirse en cualquier medio físico o tecnológico. Se entenderá por mensaje de datos a la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o de cualquier otra tecnología.

## **Título Decimotercero.- Delitos Contra la Paz y Seguridad de las Personas.**

### **Capítulo I Amenazas**

Artículo 282.- ...

I. ...

II. ...

III. Amenace, intimide, o cause temor a personas físicas o morales, a través de mensajes de datos, el uso de sistemas o equipos informáticos u otros mecanismos tecnológicos similares sin menoscabo de incurrir en abuso de equipos o sistemas informáticos.

...

## **Título Vigésimo Segundo.- Delitos en contra de las Personas en su Patrimonio.**

### **Capítulo I. Robo**

Artículo 368.- Se equiparan al robo y se castigarán como tal:

I. ...

II. ...

III. La copia, sustracción o el apoderamiento de información contenida en sistemas o equipos informáticos, o el aprovechamiento o utilización de dicha información sin derecho y sin consentimiento de la persona que legalmente pueda disponer de la misma.

## **Título Vigésimo Segundo.- Delitos contra las personas en contra de su patrimonio**

### **Capítulo III.- Fraude**

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

## **Título Vigésimo Sexto.- De los Delitos en Materia de Derecho de Autor.**

### **Capítulo Único**

Artículo 424 bis.- Se impondrá prisión de tres a diez años y de dos mil a veinte mil días multa a quien produzca, reproduzca, introduzca al país, almacene, transporte, distribuya, venda o arriende copias de obras, fonogramas, videogramas y libros protegidos por la Ley Federal del Derecho de Autor; en forma dolosa, con fin de especulación comercial y sin la autorización que en los términos de la citada Ley deba otorgar el titular de los derechos de autor o de los derechos conexos.

Artículo 426.- Se impondrá prisión de seis meses a cuatro años y de trescientos a tres mil días multa, a quien descifre por sí solo o a través de un sistema o equipo informático una señal de satélite protegida por algún mecanismo de seguridad sin autorización de su distribuidor.

Igual pena se impondrá a quienes, a sabiendas, aporten o provean de cualquier forma, materias primas o insumos destinados a cometer las conductas a que se refiere el párrafo anterior.

## **Título Vigésimo Séptimo.- Delitos Cibernéticos**

### **Capítulo I Definiciones**

Artículo 430.- Para los efectos de este título y aquellas disposiciones de este código que contemplen las siguientes definiciones, adicionalmente, se entenderán de la siguiente forma:

I. Sistemas o equipos informáticos: cualesquiera conjuntos o unidades de máquinas, aparatos, sistemas, equipos de informática o en general cualquier dispositivo, ya sea electrónico, óptico, magnético, o de cualquier otra tecnología, que realice funciones lógicas, aritméticas, transmisión, procesamiento o almacenamiento de datos de cualquier naturaleza, así como para el tratamiento sistemático de la información mediante el procesamiento automático de datos electrónicos o de cualquier otra tecnología.

II. Programas de cómputo o computación: la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que un sistema o equipo informático realice una tarea o función específica.

III. Daño: alteración, deterioro o menoscabo a la integridad, confidencialidad o disponibilidad de datos, información o programas de cómputo, así como la destrucción, descompostura, deterioro o menoscabo físicos causado a sistemas o equipos informáticos.

IV. Mensajes de datos: la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o de cualquier otra tecnología.

Información: archivos, imágenes, sonido, video, símbolos o datos de cualquier índole, así como documentos que consten o sean susceptibles de reproducirse en cualquier medio físico o tecnológico, o cualquier registro que conste la comisión de un delito, sin importar su fuente o fecha de elaboración.

VI. Mecanismo de seguridad: dispositivo físico o electrónico, palabra clave, código de acceso, programa de cómputo o equipo informático que tenga por objetivo proteger una computadora, un programa de cómputo o la información contenida en un, sistema o equipo informático contra:

- a) Accesos internos o externos no autorizados;
- b) Borrado, alteración o daño de información;
- c) Ataque informático de cualquier índole;
- d) Rechazo del emisor, receptor o destinatario de la información.
- e) Copiado, distribución, uso ilícito o no autorizado.

VII. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, correo electrónico, firma electrónica, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

## Capítulo II

### Acceso no Autorizado a Sistemas o Equipos Informáticos.

Artículo 431.- Comete el delito de acceso no autorizado a sistemas o equipos informáticos o programas de computación, la persona que sin derecho:

I. Acceda a información o a un sistema o equipo informático sin autorización o excediendo su acceso autorizado;

II. Intercepte, modifique, borre, destruya, provoque daño o pérdida de información contenida en sistemas o equipos informáticos o programas de cómputo;

III. Conozca, copie, divulgue o distribuya hacia terceros información o comunicaciones no dirigidas a él contenidas en sistemas o equipos informáticos;

IV. Diseñe, introduzca, programe, distribuya, o provoque la transmisión o ejecución de programas de computación, información, códigos, conjuntos de instrucciones o comandos informáticos, que tengan por objeto:

a) Impedir el uso, funcionamiento apropiado, o causar daños a información contenida en sistemas o equipos informáticos, o programas de computación;

b) Alterar la información de programas de computación contenidos en sistemas o equipos informáticos o, y

c) Causar la negación de servicios de naturaleza informática realizados por sistemas o equipos informáticos, o programas de computación.

V. Para violar mecanismos de seguridad de sistemas o equipos informáticos, o programas de cómputo: diseñe, programe, importe, fabrique, posea, use, comercialice, transmita, haga disponibles hacia terceros o distribuya; máquinas, aparatos, sistemas, equipos o cualquier dispositivo físico, así como programas de cómputo, números de serie o registro, palabras clave o códigos de acceso, o información de cualquier naturaleza;

VI. Produzca, copie, posea, trafique, transmita, difunda, distribuya o haga disponible hacia terceros a través de sistemas o equipos informáticos, de sus redes, de dispositivos de almacenamiento magnéticos, ópticos, electrónicos o de cualquier otra tecnología:

a) Pornografía de menores;

b) Lenocinio de menores;

c) Información xenofóbica, racista o discriminatoria de cualquier naturaleza;

d) Incitaciones o provocaciones para cometer delitos de cualquier índole, e

e) Información que explique cómo realizar cualesquiera de los delitos contemplados en este capítulo.

VII. Obtenga sin consentimiento, o mediante engaños, datos personales de individuos para usarlos para cometer cualquier actividad ilícita;

VIII. Transmita, distribuya o haga disponible a través de sistemas o equipos informáticos datos personales de terceros sin su consentimiento;

IX. Inserte, altere, o elimine información veraz contenida en sistemas o equipos informáticos o programas de cómputo, lo cual resulte en información falsa aparentemente auténtica, independientemente de si la información sea directamente legible o accesible para su consulta, y

X. Cause daño físico, mediante cualquiera de los actos u omisiones descritos en las fracciones anteriores, a sistemas o equipos informáticos, redes de sistemas o equipos informáticos, equipos periféricos, o cualquier otro bien tangible.

Se perseguirá a querrela de parte ofendida, salvo los casos previstos en la fracción V, los incisos a) y b) de la fracción VII, las agravantes mencionadas en la fracción II, los incisos b) y c) de la fracción III del artículo 433, y las previstas en el artículo 434; en cuyo caso serán de oficio.

Artículo 432.- Se impondrán las siguientes penas respecto a las fracciones del artículo anterior que a continuación se describen:

I. De 1 - 3 años de prisión y de 100 - 400 días de multa para las fracciones I y III ;

II. De 2 - 5 años de prisión y de 300 - 700 días de multa para las fracciones II, VI, VII y VIII;

III. De 5 -10 años de prisión y de 600 -1000 días de multa para las fracciones IV, V, IX y X.

Artículo 433.- Las penas previstas en el artículo anterior se aumentarán hasta en una mitad

I. Para los casos previstos en las fracciones III y V, cuando la información obtenida se utilice en beneficio propio o ajeno;

II. Para el caso previstos en la fracción IV, cuando el daño se haya extendido masivamente, afectando a sistemas o equipos informáticos localizados en varias Entidades Federativas.;

III. Para todas las fracciones del artículo 431:

a) Cuando las conductas sean cometidas por funcionarios, empleados o personas que presten sus servicios en la institución, organización o empresa víctima del delito;

b) Cuando el delito se haya cometido en contra de sistemas o equipos informáticos de gobierno o del sistema financiero;

c) Cuando dos o más individuos hayan actuado coordinadamente para perpetrar alguno de los delitos de este título;

d) Cuando para cometer el delito se haya violado algún mecanismo de seguridad;

e) Cuando con el fin de disimular su identidad o ubicación, se haya aprovechado de sistemas o equipos informáticos o datos personales de un tercero, o haya usado datos falsos para realizar cualesquiera de las conductas tipificadas en este capítulo;

f) Cuando bajo engaños o aprovechándose del error en que se encuentra una persona, obtiene de ésta información, códigos o claves de acceso, o logra instalar en sistemas o equipos informáticos programas de cómputo de terceros, que le permitan realizar cualesquiera de las conductas tipificadas en este capítulo.

Artículo 434.- Las penas previstas en este capítulo se aumentarán hasta el doble, cuando se hayan dado dos o más agravantes contempladas en el artículo 433; o cuando el delito informático haya sido motivado por cuestiones políticas, interés de grupo; o que impliquen los delitos que se señalan en el Título Primero del presente Libro.

Artículo 435.- Las penas previstas en las fracciones I, II y III del artículo 431 disminuirán entre la mitad y dos terceras partes si el delito fuese culposo o si de él no se derivó ningún daño o perjuicio de cualquier índole.

### **Capítulo III**

#### **Abuso de Sistemas o Equipos Informáticos.**

Artículo 436.- Comete el delito de abuso de sistemas o equipos informáticos, la persona física o moral que aproveche sistemas o equipos informáticos para la comisión de cualquier delito distinto a este capítulo o aquellos contemplados en las leyes especiales.

Para sancionar esta conducta se impondrá hasta la mitad de la pena correspondiente al delito con el que concurra.

### **Capítulo IV**

#### **Disposiciones Generales para los Capítulos de este Título**

Artículo 437.- Las conductas previstas en el presente Título únicamente podrán ser atribuidas a un Proveedor de Acceso a Internet, en los casos siguientes:

- I. En la medida en que sus dispositivos de transmisión o almacenamiento automático, provisional y temporal de información, en los cuales se tipifica el delito, estén bajo su control o estas conductas se lleven a cabo de forma personal y directa por dicho proveedor o sus representantes;
- II. Si al conocer el contenido ilegal de la información omite retirar o bloquear inmediatamente el acceso a esta;
- III. Si crea o modifica la información ilegal transmitida, o elige a los destinatarios de dicha información.

Responsabilidades adicionales de los proveedores de servicios de telecomunicaciones estarán señaladas en la ley de la materia.

Artículo 438.- Cuando de la comisión de los delitos a que se refiere el presente capítulo resultaren otros delitos, se estará a las reglas del concurso.

**Artículo Segundo.- Se reforman del Código Federal de Procedimientos Penales los artículos 175 del Capítulo Primero y 194 del Capítulo Quinto, ambos del Título Quinto; del Título Sexto los artículos 268 bis del Capítulo Séptimo y el artículo 285 del Capítulo Noveno; lo anterior, para quedar como sigue:**

#### **Título Quinto.- Disposiciones Comunes a la Averiguación Previa y a la Instrucción**

### **Capítulo I**

#### **Comprobación del Cuerpo del Delito y de la Probable Responsabilidad del Inculpado.**

Artículo 175.- Tratándose de delitos informáticos para la comprobación del cuerpo del delito y la probable responsabilidad del indiciado se tomarán en cuenta: clase o tipo de sistema o equipo informático utilizado, la información contenida en ellos como evidencia o prueba del ilícito y los conocimientos técnicos o profesionales del indiciado en materia informática o en el manejo del sistema o equipo en cuestión.

### **Capítulo IV**

#### **Aseguramiento del Inculpado**

Artículo 194.- ...

I. ...

1) a 12) ...

13) Corrupción de menores o de Personas con capacidades diferentes, pornografía y lenocinio infantiles previstos en los artículos 201, 202 y 204, respectivamente;

14) Los previstos en los artículos 204 y 206;

15) a 33) ...

II. a la XIV. ...

## **Título Sexto.- Prueba**

### **Capítulo VII.**

#### **Careos**

Artículo 268 bis.- Cuando la víctima u ofendido sea menor de dieciocho años o no tenga capacidad para comprender el significado del hecho, las declaraciones que se reputen contradictorias se practicarán en la misma forma que el careo supletorio.

### **Capítulo IX**

#### **Valor Jurídico de la Prueba**

Artículo 285.- Todos los demás medios de prueba o de investigación y la confesión, salvo lo previsto en el artículo 175, constituyen meros indicios.

**Artículo Tercero.- Se reforman las siguientes disposiciones de la Ley Federal contra la Delincuencia Organizada: el artículo 2 del Capítulo Único en el Título Primero; del Título Segundo, Capítulo Cuarto, los artículos 20, 22 y 23; lo anterior para quedar como sigue:**

## **Título Primero.- Disposiciones Generales**

### **Capítulo Único**

#### **Naturaleza, Objetos y Aplicación de la Ley**

Artículo 2.- ...

I. a la IV. ....

V. Pornografía de menores, lenocinio en la misma modalidad, o trata de menores, o de personas que no tienen capacidad para comprender el significado del hecho, previstos en los artículos 201, 202, 204 y 206; asalto, previsto en los artículos 286 y 287; secuestro, previsto en el artículo 366; tráfico de menores, previsto en el artículo 366 ter y robo de vehículos, previsto en el artículo 381 bis, todos del Código Penal Federal o en las disposiciones equivalentes de las legislaciones penales del Distrito Federal y de los Estados de la República integrantes de la Federación.

## **Título Segundo.- De la Investigación de la Delincuencia Organizada**

### **Capítulo Cuarto**

#### **De las Órdenes de Cateo y de Intervención de Comunicaciones**

Artículo 20.- Durante las intervenciones de las comunicaciones privadas, el Ministerio Público de la Federación ordenará la transcripción de aquellas grabaciones que resulten de interés para la averiguación previa y las cotejará en presencia del personal del cuerpo técnico de control de la unidad especializada prevista en el artículo 8o. anterior, en cuyo caso serán ratificadas por quien las realizó. La transcripción contendrá los datos necesarios para identificar el *dispositivo óptico electrónico o magnético* de donde fue tomada. Los datos o informes impresos que resulten de la intervención serán igualmente integrados a la averiguación.

Las *secuencias* o imágenes de video que se estimen convenientes podrán, en su caso, ser convertidas a imágenes fijas para ser impresas e integrarlas a la indagatoria. En este caso, se indicará el *dispositivo* de donde proviene la imagen y el nombre y cargo de la persona que realizó la conversión.

Artículo 22.- De toda intervención se levantará acta circunstanciada por el Ministerio Público de la Federación, que contendrá las fechas de inicio y término de la intervención; un inventario pormenorizado de los documentos, objetos y los *dispositivos ópticos, electrónicos o magnéticos* para audio o video que contengan los sonidos o imágenes captadas durante la misma; la identificación de quienes hayan participado en las diligencias, así como los demás datos que considere relevantes para la investigación. *Los dispositivos originales y el duplicado de cada una de ellos*, se numerarán progresivamente y contendrán los datos necesarios para su identificación. Se guardarán en sobre sellado y el Ministerio Público de la Federación será responsable de su seguridad, cuidado e integridad.

Artículo 23.- Al iniciarse el proceso, *los dispositivos ópticos, electrónicos o magnéticos*, así como todas las copias existentes y cualquier otro resultado de la intervención serán entregados al juez de distrito. Durante el proceso, el juez de distrito, pondrá *los dispositivos* a disposición del inculpado, *quien accederá a la información contenida en ellos para escucharla o verla* durante un periodo de diez días, bajo la supervisión de la autoridad judicial federal, quien velará por la integridad de estos elementos probatorios. Al término de este periodo de diez días, el inculpado o su defensor, formularán sus observaciones, si las tuvieran, y podrán solicitar al juez la destrucción de *aquellos dispositivos, información* o documentos no relevantes para el proceso. Asimismo, podrá solicitar la transcripción de aquellas grabaciones o la fijación en impreso de imágenes o *secuencias de video*, que considere relevantes para su defensa.

La destrucción también será procedente cuando *los dispositivos, la información* o los registros provengan de una intervención no autorizada o no se hubieran cumplido los términos de la autorización judicial respectiva.

El auto que resuelva la destrucción de *dispositivos*, la transcripción de grabaciones o la fijación de imágenes, es apelable con efecto suspensivo.

**Artículo Cuarto.- Se modifica el inciso a), numeral III, del artículo 4 del Capítulo Segundo correspondiente a la Ley de la Policía Federal Preventiva; para quedar como sigue:**

## **Capítulo II**

### **De la Organización y Funcionamiento de la Institución**

Artículo 4.- ...

I. ...

II. ...

III. ...

a) Las zonas fronterizas y en la tierra firme de los litorales, la parte perteneciente al país de los pasos y puentes limítrofes, las aduanas, recintos fiscales, secciones aduaneras, garitas, puntos de revisión aduaneros, los centros de supervisión y control migratorio, las carreteras federales, las vías férreas, los aeropuertos, los puertos marítimos autorizados para el tráfico internacional, los medios de transporte que operen en las vías generales de comunicación así como sus servicios auxiliares, y *las redes públicas de telecomunicaciones*

b) a d) ...

IV. a la XV. ...

## **Transitorios**

**Primero.-** El presente decreto entrará en vigor al día siguiente de su publicación.

**Segundo.-** La Policía Federal Preventiva deberá formalizar en 60 días, la creación de la Unidad de Policía Cibernética.

**Tercero.-** La Policía Federal Preventiva a través de su Policía Cibernética, será responsable de la capacitación a los órganos administrativos y judiciales en materia penal respecto a delitos cibernéticos. Podrá capacitar y coordinar a los cuerpos policíacos estatales especializados en esta materia, así como impulsar su creación en aquellas entidades que carezcan de éstos, respetando los esquemas de coordinación de seguridad pública entre autoridades federales y estatales.

**Cuarto.-** Se formalizará el convenio de colaboración que da origen al Grupo Interinstitucional para combatir los Delitos Cibernéticos, en los mismos términos como actualmente se desempeña, para cumplir trabajos de consultoría y asesoría respecto a las políticas públicas de combate al delito cibernético, así como otras conductas que causen un perjuicio social por el uso de redes de telecomunicaciones públicas o privadas incluyendo Internet.

**Quinto.-** La persecución de los delitos cibernéticos y aquellos que tengan que ver con sistemas o equipos informáticos a que se refieren las legislaciones modificadas, será responsabilidad de las autoridades federales, estatales y municipales conforme a los convenios de coordinación en materia de seguridad pública que hayan sido suscritos entre sí. Asimismo se buscará la colaboración con autoridades internacionales cuando los delitos tengan éste carácter, de conformidad a los tratados y convenios de cooperación internacionales celebrados para tal efecto.

Dado en Palacio Legislativo de San Lázaro, a los 12 días del mes de abril de 2005.

**Nota:**

1 Eduardo García Maynez. Introducción al Estudio del Derecho, pág. 27, Ed. Porrúa, México 1992.

Dip. Sheyla Fabiola Aragón Cortés (rúbrica)