

CONGRESO DE LA REPÚBLICA  
GUATEMALA, C. A.

**DIRECCIÓN LEGISLATIVA**  
**- CONTROL DE INICIATIVAS -**

NÚMERO DE REGISTRO

**6236**

**FECHA QUE CONOCIÓ EL PLENO: 06 DE SEPTIEMBRE DE 2023.**

**INICIATIVA DE LEY PRESENTADA POR LOS REPRESENTANTES OSCAR STUARDO CHINCHILLA GUZMÁN Y YESMIN MARÍA POROJ ORELLANA.**

**INICIATIVA QUE DISPONE APROBAR REFORMA AL CÓDIGO PENAL, DECRETO NÚMERO 17-73 DEL CONGRESO DE LA REPÚBLICA.**

**TRÁMITE: PASE A LA COMISIÓN DE REFORMAS AL SECTOR JUSTICIA, PARA SU ESTUDIO Y DICTAMEN CORRESPONDIENTE.**



**RECIBIDO**  
18 ABR 2023

FIRMA \_\_\_\_\_ HORA 10:10

**INICIATIVA NUEVA**

**EXPOSICIÓN DE MOTIVOS**

**HONORABLE PLENO:**

**ANTECEDENTES**

Actualmente Guatemala no cuenta con legislación especial que regule normas relativas a los delitos informáticos cometidos a través de sistemas que utilicen tecnologías de la información, únicamente se encuentran algunas normas que fueron adicionadas a nuestro actual Código Penal, mismas que no responden a las necesidades actuales, debido a la irrefutable variación de las tecnologías de la información, lo que obliga a actualizar las normas de dicha normativa con la finalidad de prevenir, sancionar y erradicar los delitos de naturaleza informática que pudieran afectar el objeto o materia de la normativa de comercio electrónico, y todos aquellos actos ilícitos de naturaleza informática, cumpliendo a cabalidad con todas las pautas y reglas a nivel internacional tomando como base el Convenio sobre la Ciberdelincuencia suscrito en Budapest con fecha veintitrés de noviembre del año dos mil uno, que ha sido la ley modelo para la regulación de cibercrimen.

La presente iniciativa establece por consiguiente, las normas especiales que sean suficientes para prevenir y sancionar las conductas de cibercrimen que no tienen fronteras, ni poseen lenguaje específico, y que se realizan en un espacio virtual o ciberespacio. Con el contenido de dicha iniciativa se pretende brindar protección integral de la información de las personas que se almacena, opera o transmite por medio de sistemas que utilizan tecnologías de la información, así como la prevención y sanción de los delitos cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas.

**AVANCE DE REGULACION DE LOS DELITOS INFORMATICOS DE GUATEMALA Y LOS PAISES DE LATINO AMERICA**

Para establecer el avance de la regulación se ha tomado en cuenta el informe “Estado situacional y perspectivas del derecho informático en América Latina y el Caribe”, que analiza la situación de la regulación en materia de Delitos Informáticos y Delitos por medio de las tecnologías de la información.

Durante varios años el desarrollo normativo ha estado focalizado en la penalización del uso de las Tecnologías de la Información (TIC), sobre todo en tema de pornografía infantil, aunque hay que indicar que se sigue el lineamiento doctrinario de que no era necesaria una regulación sino una adecuada formación de los jueces y actores jurídicos relacionados en interpretar las normativas existentes.

Sin embargo hay que indicar que esta serie de legislaciones se encuentran con problemas de persecución por parte de las fuerzas de la ley que no tienen formación en la materia o se encuentran en sus fases iniciales del establecimiento de las normas que regulen este



tipo de delitos en contra de la ciberdelincuencia, por lo que se hace necesario que se inicie por parte del Estado de Guatemala la adecuación de la normativa correspondiente.

Debemos tomar en cuenta el aumento de la penetración de Internet, ya que es un factor que sirve como detonante para analizar y plantear adecuadamente la regulación legal en la materia, sin embargo no será hasta que se logre la adopción de leyes y reglamentos para que realmente avance adecuadamente, y lo mismo pasa por la diversidad de definiciones que se tienen hacia lo que es un delito informático. La presente iniciativa es precisamente un conjunto de factores que buscan combatir los crímenes informáticos.

Es preciso hacer mención que se ha tomado en cuenta diversos criterios que sirven de base para la presente iniciativa de ley a nivel de Latino América tal el caso de los conceptos de la declaración de cibercrimen y lo dispuesto en la Asamblea General de la Organización de Estados Americanos (OEA) de fecha ocho de junio del dos mil cuatro, lo cual queda reflejado en la presente iniciativa de ley, una legislación avanzada que considera los mejores procesos normativos de la Región para ser aplicados dentro de nuestra normativa interna y regular drásticamente las penas y sanciones en contra de los delitos relacionados con el tema.

La iniciativa busca la uniformidad sustancial y procesal de las normas penales ya determinadas en nuestro país y analizar a su vez las necesidades que sobre el avanzado tema de cibercrimen existe hoy en día, tomando en cuenta los asuntos presentes y futuros que van día con día creándose de una manera impredecible, razón por la cual se consideraron los siguientes puntos:

- a) Que es necesario proteger a la sociedad frente a la amenaza de los delitos cometidos por vía informática.
- b) La naturaleza volátil de estos delitos crea la necesidad de buscar mecanismos de cooperación nacional e internacional claros y funcionales.
- c) Es necesario garantizar a la sociedad la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y de los sistemas que utilicen tecnologías de la información y comunicación.
- d) Se hace necesario crear, capacitar y dotar de tecnología a Organismos del Estado que manejen la seguridad especializada en sistemas informáticos y de los sistemas que utilicen tecnologías de la información y comunicación.
- e) Es necesaria la participación activa de nuestro país en actividades relacionadas con la ciberdelincuencia, de manera que tengamos la capacidad de detectar vulnerabilidades, generar soluciones, generar las propias herramientas técnicas y estrategias de investigación.

El Convenio del Consejo de Europa ha definido cuatro categorías de delitos informáticos, entiéndase cualquier acto cometido dentro del uso de las tecnologías de la información y comunicación, siendo estas las siguientes:



1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos.
2. Delitos estrictamente informáticos.
3. Delitos relativos al contenido.
4. Delitos relativos a la violación de los derechos de autor y derechos afines.

Cabe manifestar, que la Unión Europea ha dado prioridad, en cuanto se refiere a estos aspectos sustanciales, a la pornografía infantil, entre otros.

Los constantes avances tecnológicos y los altos niveles de conocimientos técnicos involucrados en los nuevos desarrollos de sistemas que utilizan tecnologías de la información y comunicación, forman un reto para presentar una definición general de lo que puede denominarse un delito por computadora. En ese sentido, existen múltiples interpretaciones y sugerencias que buscan modelar esta naciente y conflictiva área para el derecho y las tecnologías de información. El no contar con una definición concreta sobre el tema desestima los esfuerzos para una adecuada detección, investigación y juzgamiento de este tipo de conductas cometidos contra éstos o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías en perjuicio de personas físicas o jurídicas.

La delincuencia informática es una realidad que requiere de iniciativas de leyes como la que hoy se presenta, en las que contienen estrategias de prevención y combate de la misma. Insinuar que la criminalidad informática es un problema jurídico, o tecnológico, o social o mercantil, sería negarnos o cerrarnos las puertas a la posibilidad de haber presentado la iniciativa de ley que lo que busca es el profundizar en las problemáticas de las vulnerabilidades, de la inseguridad de los individuos a nivel de la informática.

#### **PROPUESTA DE REGULACION LEGAL, CONTENIDO EN EL CONVENIO DE BUDAPEST**

El Convenio sobre la Ciberdelincuencia es un tratado internacional suscrito en Budapest el 23 de noviembre del 2001, por los miembros del Consejo de Europa COE, para incrementar la cooperación entre los funcionarios de las instituciones policiales de diferentes países. El Convenio de Budapest fue oficialmente redactado por los 43 países miembros del Consejo de Europa, junto con los EE UU., Canadá, Japón y otros que participaron como observadores.

Mediante el Convenio de Budapest se propone fundamentalmente incluir una relación de delitos que cada Estado miembro debe considerar como tales. El tratado tipifica como delitos a las infracciones de piratería, la producción, venta o distribución de herramientas de piraterías, la pornografía infantil y una lista amplia de infracciones de la propiedad intelectual (Artículos 2-11).

De acuerdo con lo previsto en el artículo 37 del Convenio, relativo a la Adhesión al mismo, aquellos países que no participaron en la elaboración del Convenio, podrán ser invitados



por el Comité de Ministros del Consejo de Europa, previa consulta y consentimiento unánime de los Estados contratantes del Convenio, para adherirse al mismo.

Por otro lado, el Capítulo IV prevé la posibilidad de que el país o países adherentes determinen el territorio donde se aplicará la convención y hagan declaraciones, reservas o enmiendas.

Una posibilidad clara para que los Países de América Latina adapten su normativa y establezcan lazos estrechos de cooperación que les permita enfrentar la ciberdelincuencia, lo constituye la adhesión al Convenio sobre la Ciberdelincuencia suscrito en Budapest en noviembre de 2001.

Dicho Convenio está abierto a la adhesión de terceros países, distintos a los que son miembros u observadores del Consejo de Europa, para ello debe mediar la invitación por parte del Comité de Ministros del Consejo de Europa, previa consulta y consentimiento unánime de los Estados Contratantes del Convenio.

Para ello, es preciso que los países manifiesten de manera inequívoca su voluntad política de ser parte del convenio y lleven a cabo una gestión diplomática al más alto nivel para que se obtenga la invitación de Ministros referida.

La base para esta propuesta se encuentra en la *Tarea Pendiente 1 de Delitos Informáticos*, del documento **“Estado situacional y perspectivas del derecho informático en América Latina y el Caribe”**, que propone el: *“(…) diseño de una propuesta normativa mínima, basada entre otros en las propuestas del tratado de Cibercrimen, ya existentes”*. Siendo así que la Convención de Cibercrimen y su Protocolo Adicional, son la base de esta propuesta de iniciativa de ley.

### **Presupuestos del Cibercrimen en la Red.**

El cibercrimen representa el estado más sofisticado de la conducta antijurídica. Esencialmente no existe mucha diferencia entre las conductas antijurídicas y punibles tradicionales con aquellas que se cometen a través de medios informáticos. Es justamente la adjetivación del delito, “informático”, la que convierte al delincuente en algo apartado de la tradición y envuelve el hecho de unas connotaciones que lo dotan de cierta autonomía conceptual. El ordenador se convierte en un instrumento del delito, no por sí solo, sino por su conexión a una red interna (intranet) o a una red externa (internet), por donde circulan usuarios, estudiantes, empresarios, profesionales, pederastas, grandes sumas de dinero encriptadas, estafadores, sabotadores, niños y terroristas.

Predominantemente existen dos formas de comunicación a través de Internet: El correo electrónico y la World Wide Web. Simplificaremos nuestra exposición ignorando otros modos de comunicación en red que han perdido protagonismo o que poseen una importancia delictiva muy limitada, como el Bulletin Board System BBS, Internet Relay Chats (IRC), Usenet, website “guest books”, weblogs, File Transfer Protocol, P2P, particulares aplicaciones como Napster, Gnutella, sin perjuicio de que gran parte de lo dicho en estas páginas sea aplicable a dichos sistemas de comunicación. Por otro lado





existe otra modalidad como la WWW, el Webcasting, que define como "grupo de servicios emergentes que utilizan Internet para la entrega de contenidos a los usuarios, de una forma muy similar a los servicios de comunicación".

La World Wide Web (WWW), es un sistema de hipertexto que funciona sobre Internet, a través del cual, y con la ayuda de una aplicación informática destinada al efecto, el navegador web, se extrae información (llamada "documentos" o "páginas web") y se muestra en la pantalla del usuario. Siguiendo los hiperenlaces, el usuario puede acceder a múltiples páginas, lo que se denomina "navegación". Dicha páginas se encuentran hospedadas en servidores donde se almacena la información en discos duros.

Es frecuente que los responsables de las páginas y portales Web utilicen vías distintas de acceso para transferir los contenidos. El más utilizado es el protocolo FTP. Del mismo modo que el conductor ebrio, para cometer un delito contra la seguridad del tráfico, necesita un vehículo a motor, drogas tóxicas o bebidas alcohólicas y, generalmente, una vía pública asfaltada como escenario, el ciberdelincuente requiere disponer de un terminal de ordenador (el vehículo a motor), una conexión a Internet (la vía pública) y las distintas estaciones que posibilitan la circulación: proveedores de servicios, de contenido, mirrors, proxys, etc. (el asfalto.)


Principalmente son tres o cuatro sujetos, como mínimo, los que participan en el fenómeno del cibercrimen. El sujeto activo del delito, que inicia la conducta punible (sea enviando contenidos a un servidor, sea descargando archivos prohibidos, sea remitiendo e-mails difamatorios); los sujetos coadyuvantes sin cuya intervención el ciberdelincuente carecería de los medios técnicos necesarios para desarrollar su conducta criminal (el servidor de acceso, que posibilita la conexión a la red y el servidor de contenidos, en cuyos discos duros se alberga la información delictiva, que más tarde ofenderá o causará perjuicios); y, por último, el sujeto pasivo del delito, caracterizado en Internet por ser plural, a veces masivo, internacional y, casi siempre, indeterminado y desconocido para el delincuente.

Generalmente, serán estos sujetos los protagonistas del cibercrimen, pero, en ocasiones, si el delito consiste en el envío directo de e-mails, no intervendría el servidor de contenidos, cifrándose en tres los participantes.

Todo lo anterior, nos conduce a presentar la presente iniciativa de Ley que contiene reformas al Código Penal, dirigido a sancionar a los responsables de los delitos que delinquen, aprovechándose de las tecnologías de la información y las comunicaciones, con miras a procurar su aprobación como Ley de la República.

**DIPUTADO (S) PONENTE (S):**

  
**OSCAR STUARDO CHINCHILLA GUZMÁN**

  
Yesmin Marta  
Poruj Orellana<sup>5</sup>.



**CONGRESO  
DE LA REPÚBLICA**  
IX LEGISLATURA

**DECRETO NÚMERO ...**

**EL CONGRESO DE LA REPÚBLICA DE GUATEMALA**

**CONSIDERANDO:**

Que conforme el texto constitucional, el Estado se organiza para proteger a la persona y a la familia, siendo su fin supremo la realización del bien común; en ese sentido, es deber del Estado garantizar a los habitantes de la República, la vida, la libertad, la justicia, la paz, su desarrollo integral, y para el caso de la norma que mediante este instrumento se aprueba por parte de este Organismo de Estado, la seguridad.

**CONSIDERANDO:**

Que es indispensable reformar el Código Penal, a efecto de legislar en procura de la protección de los derechos de toda persona en cuanto a su integridad, disponibilidad y confidencialidad de los sistemas que utilicen tecnologías de la información y sus componentes, a fin de garantizar certeza jurídica, armonizar y contribuir con las disposiciones internacionales con relación a la prevención y sanción de los delitos informáticos.

**CONSIDERANDO:**

Que para poder contrarrestar los ataques cibernéticos, el Estado de Guatemala debe emitir normas especiales en materia de delitos informáticos, toda vez que, por la naturaleza de los actos de cibercrimen, que a su vez se trata en algunos casos de delitos transfronterizos, se complica la aplicación de las actuales normas del Código Penal, lo que se traduce en lagunas legales que permite a quienes se dedican a realizar actos ilícitos, aprovecharse de las nuevas tecnologías de la información, por lo que las disposiciones que han de emitirse deben ser congruentes con la normativa internacional.

**POR TANTO:**

En ejercicio de las atribuciones que le confiere el inciso a) del artículo 170 de la Constitución Política de la República de Guatemala,

**DECRETA:**

Las siguientes:

**REFORMAS AL CÓDIGO PENAL,  
DECRETO NÚMERO 17-73 DEL CONGRESO DE LA REPÚBLICA**

**Artículo 1.** Se adiciona el artículo 190 quater, el cual queda así:

**“Artículo 190 quater. Engaño con fines sexuales.** Comete el delito de engaño con fines sexuales, quien valiéndose o no del anonimato, contacte a un niño, niña o adolescente, utilizando sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, con el



objetivo de ganarse su confianza por cualquier método, para proponerle concertar un encuentro en un lugar físico, con la intención de cometer cualquier delito que atente contra su libertad o indemnidad sexual, incluso aunque no se haya llevado a cabo un contacto corporal entre el sujeto activo y la víctima.

El responsable de este delito será sancionado con prisión de cinco a ocho años de prisión y multa de doscientos a seiscientas veces el salario mínimo legal vigente para actividades no agrícolas.

Además de las agravantes contempladas en el presente Código, la pena de prisión será de seis a nueve años en los siguientes casos:

- a) Si la víctima, por su condición, fuera colocada en situación de total indefensión; y en todo caso, cuando sea menor de trece años;
- b) Cuando la violencia o intimidación ejercidas por el sujeto activo revistan un carácter particularmente degradante o vejatorio;
- c) Cuando el sujeto activo fuere pariente de la víctima, o responsable de su educación, guarda, custodia, cuidado, tutela; se trate de pariente dentro de los grados de ley, o tenga una condición de superioridad, o sea afín con la víctima;
- d) Cuando el autor del delito haya puesto en peligro la vida del niño, niña o adolescente;
- e) Cuando se trate de delincuencia organizada.

La pena será aumentada en dos terceras partes, cuando la víctima sea un niño, niña o adolescente con incapacidad cognitiva o volitiva.

La pena se impondrá sin perjuicio de las que puedan corresponder por la comisión de otros delitos."

**Artículo 2.** Se adiciona el artículo 274 bis, el cual queda así:

**“Artículo 274 bis. Acceso ilícito al uso de tecnologías de la información y las comunicaciones.** Comete el delito de acceso ilícito al uso de tecnologías de la información, quien de forma deliberada, sin autorización o excediendo la que posea, acceda a sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones. El responsable de este delito será sancionado con prisión de dos a cuatro años y multa de cien a quinientas veces el salario mínimo legal vigente para actividades no agrícolas.

La pena será de tres a seis años de prisión y multa de doscientas a setecientas veces el salario mínimo legal vigente para actividades no





agrícolas, en los siguientes casos:

- a) Cuando para acceder al sistema informático o sistemas que utilicen las tecnologías de la información y las comunicaciones, se suplante la identidad del destinatario o del remitente;
- b) Cuando se utilicen programas, equipos, materiales o dispositivos para obtener acceso al sistema informático o sistemas que utilicen las tecnologías de la información y las comunicaciones, o cualquiera de sus componentes, con la finalidad de ofrecer a terceros, servicios que estos sistemas proveen sin pagarlos a los proveedores de dichos servicios;
- c) Cuando el acceso se realice al generar, copiar, grabar, capturar, utilizar, alterar, divulgar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, o falsificando cualquier tipo de dispositivo de acceso al mismo;
- d) Cuando se utilicen programas, equipos, materiales o dispositivos para obtener acceso a equipos, sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, o cualquiera de sus componentes, haciendo uso no autorizado de los mismos, para procesar o realizar cualquier tipo de acción no autorizada por el propietario o legítimo usuario.”

**Artículo 3.** Se adiciona el artículo 274 ter, el cual queda así:

**“Artículo 274 ter. Acceso ilícito a datos con información protegida.**  
Comete el delito de acceso ilícito a datos con información protegida:

- a) Quien sin autorización o excediendo la que posee, se apodere o se apropie de un dato personal, datos informáticos sensibles o información confidencial de carácter personal, familiar o comercial, contenidos en sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, de naturaleza pública o privada.
- b) Quien sin autorización o excediendo la que pose, se apodere o se apropie de un dato personal, datos informáticos sensibles o información confidencial de carácter personal, familiar o comercial, contenidos en archivos o registros de naturaleza pública y que por disposición de ley o de la Constitución Política de la República de Guatemala sean de carácter confidencial, reservado o sensible.



Al responsable de este delito se le impondrá pena de prisión de cuatro a seis años y multa de cuarenta a doscientos salarios mínimos mensuales vigentes.

Quedan expresamente excluidos de la aplicación de esta disposición, y por consiguiente no podrán ser objeto de persecución penal, los casos de libertad de expresión reconocidos en la Constitución Política de la República y en los instrumentos internacionales en materia de derechos humanos de los que el Estado de Guatemala forma parte.”

**Artículo 4.** Se adiciona el artículo 274 quater, el cual queda así:

**“Artículo 274 quater. Interceptación ilícita de datos informáticos.** Comete el delito de interceptación ilícita de datos informáticos, quien de forma deliberada, sin autorización o excediendo la que posea, intercepte por cualquier medio datos informáticos, sea que éstos provengan de transmisiones restringidas, dirigidas u originadas en un sistema informático o sistemas que utilicen las tecnologías de la información y las comunicaciones, incluidas las emisiones electromagnéticas provenientes o efectuadas dentro del mismo, o del transporte de dichos datos informáticos. El responsable de este delito será sancionado con prisión de seis a diez años y multa desde cien hasta un mil veces el salario mínimo legal vigente para actividades no agrícolas.

La pena se aumentará en una tercera parte cuando la interceptación se cometa desde un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones conectado a otro sistema de la misma naturaleza.”

**Artículo 5.** Se adiciona el artículo 274 quinquies, el cual queda así:

**“Artículo 274 quinquies. Ataque a la integridad de los datos.** Comete el delito de ataque a la integridad de los datos, quien de forma deliberada, sin autorización o excediendo la que posea, dañe, borre, deteriore, modifique, altere o suprima datos informáticos y/o registros informáticos. El responsable de este delito será penado con prisión de cinco a siete años y multa desde cien hasta doscientos cincuenta veces el salario mínimo legal vigente para actividades no agrícolas.

Cuando los actos descritos en el párrafo anterior se realicen con datos informáticos relacionados con actividades comerciales o financieras, activos o pasivos bancarios, o con los estados contables o la situación patrimonial de personas físicas o jurídicas, la pena de prisión será de seis a ocho años y multa desde doscientos hasta quinientas veces el salario mínimo legal vigente para actividades no agrícolas.

Se sancionará con prisión de siete a diez años y multa de cuatrocientos a



ochocientas veces el salario mínimo legal vigente para actividades no agrícolas, cuando se tratare de datos informáticos relacionados con sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, referente o conectado a servicios públicos, registros oficiales, registros tributarios o sistemas protegidos.

Cuando el ataque sea dirigido a datos personales o personales sensibles que se encuentren en archivos, ficheros, soportes informáticos o electrónicos de instituciones públicas, se estará a lo dispuesto en la ley de acceso a la información pública.

Si la acción contemplada en los párrafos anteriores estuviere destinada a obstaculizar una investigación o procesamiento de carácter penal, el responsable será sancionado conforme al artículo 458 Bis del presente Código.”

**Artículo 6.** Se adiciona el artículo 274 sexties, el cual queda así:

**“Artículo 274 sexties. Falsificación informática.** Comete el delito de falsificación informática quien mediante cualquier medio copie, altere, sustituya deliberada e ilegítimamente datos informáticos de un sistema que haga uso de las tecnologías de la información y las comunicaciones o uno de sus componentes, generando un resultado no auténtico o tenga por finalidad inducir a usuarios a proporcionar datos confidenciales, bancarios y/o financieros. El responsable de este delito será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente para actividades no agrícolas.

La pena se aumentará en una tercera parte, si la intención es que el resultado sea utilizado a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.”

**Artículo 7.** Se adiciona el artículo 274 septies, el cual queda así:

**“Artículo 274 septies. Fraude informático.** Comete el delito de fraude informático quien para obtener algún beneficio para sí mismo o para un tercero, mediante cualquier artificio tecnológico o manipulación de sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones, o a sus componentes, procure la transferencia no autorizada de cualquier activo patrimonial en perjuicio de otro. El responsable de este delito será penado con prisión de cuatro a ocho años y multa desde cien hasta mil veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 8.** Se adiciona el artículo 274 octies, el cual queda así:

**“Artículo 274 octies. Apropiación de identidad ajena.** Comete el delito



de apropiación de identidad ajena, quien de forma deliberada usurpe, falsifique, adopte o suplante la identidad de otra persona individual o jurídica a través de un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones. El responsable de este delito será penado con prisión de dos a cuatro años y multa desde cuarenta hasta cien veces el salario mínimo legal vigente para actividades no agrícolas.

Cuando la comisión de este delito se realice infringiendo medidas de seguridad, se sancionará con pena de prisión de tres a cinco años y multa desde cuarenta hasta doscientos veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 9.** Se adiciona el artículo 274 nonies, el cual queda así:

**“Artículo 274 nonies. Violación a la disponibilidad.** Comete el delito de violación a la disponibilidad, quien por cualquier medio provoque a las personas que están legitimadas para hacerlo, la denegación de acceso a redes, información y sistemas que utilicen las tecnologías de la información y las comunicaciones. El responsable de este delito será penado con prisión de seis a diez años y multa desde cien a quinientas veces el salario mínimo legal vigente para actividades no agrícolas.

Cuando se deniegue la confirmación de identidad del destinatario o del remitente, ocasionando repudiación de los sistemas a las personas que están autorizadas o legitimadas para hacerlo, la pena de prisión se elevará de doce a quince años y multa desde doscientas hasta ochocientas veces el salario mínimo legal vigente para actividades no agrícolas.

Igual pena se aplicará cuando la denegación de acceso sea provocada por el envío masivo de mensajes electrónicos, publicitarios o de cualquier otra índole.”

**Artículo 10.** Se adiciona el artículo 274 decies, el cual queda así:

**“Artículo 274 decies. Abuso de dispositivos.** Comete delito de abuso de dispositivos quien, sin autorización o excediendo la que posea, cometiere cualquiera de los actos siguientes:

- a) Produzca, venda, obtenga para su utilización, importe, difunda o de cualquier otra forma ponga a disposición:
  - i. Cualquier dispositivo o programa informático, o la combinación de ambos, concebidos o adaptados principalmente para la comisión de cualquiera de los delitos previstos en los artículos 274 bis al 274 nonies del presente Código;



- ii. Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones, con la intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 274 bis al 274 nonies del presente Código.
- b) Posea alguno de los elementos contemplados en los incisos i) o ii) de la literal a) del presente artículo, con la intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 274 bis al 274 nonies del presente Código;
- c) Cree, utilice, altere, capture, grabe, copie o transfiera de un dispositivo de acceso a un medio u otro similar, o cualquier instrumento destinado a los mismos fines, códigos de identificación y acceso al servicio o sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones, que permita la operación paralela, simultánea o independiente de un servicio o sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones legítimamente obtenido por un tercero; o bien, con la intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 274 bis al 274 nonies del presente Código.

A los responsables de la comisión de este delito se les sancionará de la manera siguiente:

- 1) Con pena de tres a siete años de prisión, para el solicitante;
- 2) Con pena de cuatro a ocho años de prisión, para el productor;
- 3) Con pena de cuatro a ocho años de prisión, para el que comercializa u ofrezca;
- 4) Con pena de tres a siete años de prisión, para el que lo utiliza.

Quando exista concurrencia de las agravantes específicas mencionadas, se aplicará la de mayor penalidad. Además de la pena de prisión que corresponda, el delito será sancionado con multa de cien a setecientas veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 11.** Se adiciona el artículo 274 undecies, el cual queda así:

**“Artículo 274 undecies. Agravantes generales.** En la comisión de los delitos informáticos contemplados en los artículos 274 bis a 274 nonies del presente Código, las penas se aumentarán en una tercera parte, en los casos siguientes:



- a) Cuando el hecho sea realizado por cualquier persona que preste o haya prestado sus servicios, directa o indirectamente a la persona física o jurídica afectada. En caso de que el delito hubiera sido realizado por empleado o funcionario público, además de la pena aplicable, será inhabilitado para ejercer funciones públicas por un período de siete a diez años;
- b) Cuando de la acción realizada resulte la denegación de acceso, supresión o la modificación de datos confidenciales, reservados o de seguridad nacional, contenidos en un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones;
- c) Cuando el acto se realice para recibir ilícitamente beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas.
- d) Quien, a sabiendas de la comisión de un hecho ilícito cometido por un tercero, obtenga beneficio pecuniario o de cualquier otra índole, ya sea propio o para terceros, o para gozar de los servicios ofrecidos a través de cualquiera de estos sistemas;
- e) Cuando el hecho cometido forma parte de una acción más amplia, que constituyan actos hostiles, de conformidad con el artículo 372 de este Código; y,
- f) Cuando el hecho cometido sea realizado para atentar contra la infraestructura dedicada al procesamiento, almacenamiento y transmisión de información y datos del Estado de Guatemala."

**Artículo 12.** Se adiciona el artículo 274 duodecimos, el cual queda así:

**"Artículo 274 duodecimos. Difusión de material racista y xenófobo mediante sistemas informáticos.** Quien haciendo uso de sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, intencionadamente difunda o ponga a disposición del público material escrito, imágenes o cualquier otra representación de ideas o teorías que propugnen, promuevan o inciten al odio, la discriminación o la violencia contra cualquier persona o grupo de personas por razón de raza, color, religión, ascendencia u origen nacional o étnico, será penado con prisión de dos a tres años y multa desde veinte hasta cien veces el salario mínimo legal vigente para actividades no agrícolas."





**Artículo 13.** Se adiciona el artículo 274 terdecies, el cual queda así:

**“Artículo 274 terdecies. Amenazas con motivación racista y xenófoba mediante uso de tecnologías de la información.** Quien haciendo uso de sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, intencionadamente amenazare a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la religión, la ascendencia o el origen nacional o étnico, o a un grupo de personas que se distinga por alguna de esas características, será penado con prisión de tres a cinco años y multa desde cincuenta hasta ciento cincuenta veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 14.** Se adiciona el artículo 274 cuaterdecies, el cual queda así:

**“Artículo 274 cuaterdecies. Insultos con motivación racista y xenofóba mediante uso de las tecnologías de información.** Quien haciendo uso de sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, intencionadamente insultare a personas por razón de su pertenencia a un grupo que se caracterice por la raza, el color, la religión, la ascendencia o el origen nacional o étnico, con el objeto de exponer a la persona o grupo de personas al odio, al desprecio o al ridículo, será penado con prisión de dos a cuatro años y multa desde veinte hasta cincuenta veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 15.** Se adiciona el artículo 274 quindecis, el cual queda así:

**“Artículo 274 quindecis. Delitos contra los intereses fundamentales y la seguridad de la Nación.** Los actos que se realicen a través de un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones, que atenten contra los intereses fundamentales y seguridad de la Nación, tales como el sabotaje, el espionaje o proveer información no autorizada, serán castigados con penas de diez a veinte años de prisión y multa de mil a diez mil veces el salario mínimo legal vigente para actividades no agrícolas.”

**Artículo 16.** Se adiciona el artículo 274 sexiesdecies, el cual queda así:

**“Artículo 274 sexiesdecies. Actos de terrorismo informático.** Todo aquel que con el uso de sistemas que utilicen tecnologías de la información, ejerza actos de terrorismo contra la infraestructura del Estado, será castigado con pena de diez a veinte años de prisión y multa de mil a diez mil veces el salario mínimo legal vigente para actividades no agrícolas.”



**Artículo 17.** Se adiciona el artículo 274 septdecies, el cual queda así:

**“Artículo 274 septdecies. Difusión y alteración de imágenes personales.** Quien sin la autorización explícita y por escrito del titular, modifique, altere, envíe, difunda, transmita o almacene imágenes de otra persona por medio de sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, para fines fraudulentos o con intención de perjudicar el honor de una persona, será sancionado con prisión de cuatro a seis años y multa de cien a trescientas veces el salario mínimo legal vigente para actividades no agrícolas.

No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos.”

**Artículo 18.** Se adiciona el artículo 274 octodecies, el cual queda así:

**“Artículo 274 octodecies. Acoso mediante el uso de tecnologías de la información o medios tecnológicos.** Comete el delito de acoso mediante el uso de tecnologías de la información o medios tecnológicos, la persona individual, grupo o grupo de delincuencia organizada, que con la intención de cometer otro ilícito, públicamente en el ámbito escolar, laboral u otro ámbito determinado, y en cualquiera de las formas de autoría establecidas en este Código, valiéndose o no del anonimato, lleve a cabo mediante un sistema informático o sistema que utilice las tecnologías de la información y las comunicaciones, uno o ambos de los supuestos siguientes:

- a) Intimide o asedie a una persona o grupo de personas con contenido falso o cruel, en posesión legítima o no del sujeto activo, ya sea con la intención de ejercer dominio sobre la víctima o para que esta realice actos contra su voluntad; o,
- b) Divulgue información confidencial de otra persona que afecten su honor o su salud física o psicológica.

Al responsable de este delito se le impondrá una pena de multa de cuarenta a quinientas veces el salario mínimo legal vigente para actividades no agrícolas.

Cuando la víctima sea niño, niña o adolescente, la sanción será de prisión de uno a dos años y una multa de veinte a doscientas veces el salario mínimo legal vigente para actividades no agrícolas.

La pena será aumentada en dos terceras partes, cuando la víctima sea un niño, niña o adolescente con incapacidad cognitiva o volitiva.

La pena se impondrá sin perjuicio de las que puedan corresponder por la comisión de otros delitos.



En caso de acoso por medios cibernéticos a nivel escolar, en el cual participen niños, niñas y adolescentes, se remitirá el suceso al juez competente con el requerimiento de que se dicte la resolución correspondiente de conformidad con la Ley de Protección Integral de la Niñez y Adolescencia, prevaleciendo el interés superior del niño.”

**Artículo 19.** Se adiciona el artículo 275 bis, el cual queda así:

**“Artículo 275 bis. Delitos y faltas en la violación de la propiedad intelectual mediante el uso de tecnologías de información o medios tecnológicos.** A los responsables de la comisión de los delitos relacionados con propiedad intelectual o relativos a derechos de autor y derechos conexos, que utilicen como plataforma sistemas informáticos o sistemas que utilicen las tecnologías de la información y las comunicaciones, se les impondrá con relación a la sanción correspondiente al delito que se hubiere cometido, la pena correspondiente aumentada en una cuarta parte. El ejercicio de la acción penal, para esos casos, estará a lo dispuesto en la Ley de Propiedad Industrial y la Ley de Derechos de Autor y Derechos Conexos, respectivamente.”

**Artículo 20. Responsabilidad civil de las personas individuales y penas accesorias.**

Las sanciones penales estipulados en el presente decreto para las diferentes figuras y tipos normados, se aplicarán sin perjuicio de las responsabilidades civiles correspondientes, y los daños y perjuicios que se pudieran generar por la comisión de los actos propios de los respectivos delitos.

Asimismo, aunado a las penas de prisión y multas señaladas, el órgano jurisdiccional competente, dependiendo del caso concreto, podrá disponer la pérdida de los dispositivos electrónicos utilizados en la comisión del delito, a favor del Ministerio Público. En todo caso deberá observarse lo dispuesto en el artículo 42 y demás normativa vinculante del Código Penal, Decreto Número 17-73, y del Código Procesal Penal, Decreto Número 51-92, ambos del Congreso de la República.

Si los responsables fueron ingenieros en sistemas, técnicos en computación, técnicos en sistemas Informáticos o sistemas que utilicen tecnologías de la información y las comunicaciones, además de la sanción antes señalada, quedarán inhabilitados para ejercer su profesión por el plazo que dure la condena y si fueren reincidentes quedarán inhabilitados a ejercer su profesión de por vida.

La reparación digna se regirá conforme las disposiciones del Decreto Número 51-92 del Congreso de la República de Guatemala, Código Procesal Penal.

**Artículo 21. Responsabilidad civil y penal de las personas jurídicas.** Además de las sanciones que se indican más adelante, las personas jurídicas son responsables civilmente de las infracciones cometidas por sus órganos, representantes, empleados o cualquier persona que preste sus servicios para dicha entidad.



La responsabilidad penal por los delitos contenidos en la presente Ley, se extiende a quienes ordenen o dispongan de su realización y a los representantes legales de las personas jurídicas que conociendo de la ilicitud del hecho y teniendo la potestad para no permitirlo, lo permitan, tomen parte en él, lo faciliten o lo encubran. La responsabilidad penal de las personas jurídicas no excluye la de cualquier persona física, autor o cómplice de los mismos hechos. Cuando las personas jurídicas sean utilizadas como medios o cubierta para la comisión de un delito, o se incurra a través de ella en una omisión punible, las mismas se sancionarán con una, varias o todas las penas siguientes:

- a) Una multa igual o hasta el doble de la contemplada para la persona física para el hecho ilícito contemplado en la presente ley;
- b) La disolución, cuando se trate de un delito sancionado en cuanto a las personas individuales o físicas se refieren con una pena privativa de libertad superior a cinco años;
- c) La prohibición, a título definitivo o por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales;
- d) La sujeción a la vigilancia por un período no mayor de cinco años;
- e) La clausura definitiva o por un período de hasta cinco años, de uno o varios de los establecimientos de la empresa, que hubieran servido para cometer los hechos imputables;
- f) La exclusión de participar en los procesos de cotización y licitación, a título definitivo o por un período no menor de cinco años;
- g) La prohibición definitiva o por un período no menor de cinco años, de participar en actividades destinadas a la captación de títulos valores;
- h) La pérdida del bien o bienes que han servido o estaban destinados a cometer la infracción, o de la cosa que es su producto, a favor del Ministerio Público; y,
- i) La publicación de la sentencia pronunciada o la difusión de ésta, sea por la prensa escrita o por otro medio de comunicación.

Asimismo, se considerará responsable civilmente a una persona jurídica cuando la falta de vigilancia o de control de su representante legal o empleado haya hecho posible la comisión de un acto ilícito previsto en la presente Ley.

**Artículo 22.** Se derogan los artículos 274 "A", 274 "B", 274 "C", 274 "E", 274 "F", 274 "G" del Código Penal, Decreto Número 17-73 del Congreso de la República.

**Artículo 23.** El presente decreto entrará en vigencia ocho días después de su publicación en el diario oficial.

**REMÍTASE...**

**EMITIDO...**