

# **Comisión de Seguridad Ciudadana, Combate y Prevención al Narcotráfico, Terrorismo y Crimen Organizado**

## **Proyecto de Ley Marco de Ciberdelincuencia**

### CAPITULO I

#### ASPECTOS GENERALES

Artículo 1. Definiciones: A los efectos de la presente Ley se entiende por:

- a) sistema informático: se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan en ejecución de un programa;
- b) datos informáticos: se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;
- c) proveedor de servicios, se entenderá:
  - i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático; y
  - ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;
- d) datos sobre el tráfico: cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.
- e) material pornográfico de personas menores de edad: toda representación escrita, visual o auditiva producida por cualquier medio, de una persona menor de edad, su imagen o su voz, alteradas o modificadas, dedicada a actividades sexuales explícitas, reales o simuladas; o toda representación, real o simulada, de las partes genitales o desnudos de una persona menor de edad con fines sexuales.
- f) Alojamiento Web: todo sitio en el ciberespacio para almacenar información, imágenes, videos, o cualquier otro contenido.
- g) Alimentar bases de datos: ingresar material pornográfico utilizando a una persona menor de edad, su identidad, su imagen o su voz, en formato escrito o audiovisual, en cualquier archivo, fichero, registro u otro conjunto estructurado de datos personales, que sean objeto de tratamiento o procesamiento, automatizado o manuales, cualquiera que sea la modalidad de su elaboración, organización o acceso.

### CAPITULO II

#### TIPOS PENALES

Artículo 2.- Estafa informática

Conducta: quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

Agravante: si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

#### Artículo 3.- Daño informático

Conducta: al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

Agravante: si la información suprimida, modificada, destruida es insustituible o irrecuperable.

#### Artículo 4.- Sabotaje informático

Conducta: al que en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

Agravante: cuando:

- a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.
- b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
- c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.
- d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

#### Artículo 5.- Suplantación de identidad.

Conducta: quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

#### Artículo 6.- Espionaje informático

Conducta: al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

#### Artículo 7.- Instalación o propagación de programas informáticos maliciosos

Conducta: quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

- a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.
- b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.
- c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.
- d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.
- e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

Agravante: Cuando el programa informático malicioso:

- i. Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.
- ii. Afecte el funcionamiento de servicios públicos.
- iii. Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.
- iv. Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.
- v. Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.
- vi. Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 8.- Suplantación de páginas electrónicas

Conducta: quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

Agravante: cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 9.- Facilitación del delito informático

Conducta: quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

Artículo 10.- Narcotráfico y crimen organizado

Conducta: cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

#### Artículo 11.- Difusión de información falsa

Conducta: quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

#### Artículo 12.- Espionaje

Conducta: quien procure u obtenga indebidamente secretos de Estado debidamente decretados relativos a la seguridad interna o externa de la nación, la defensa de la soberanía nacional y las relaciones exteriores de Costa Rica.

Agravante: cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

### CAPITULO III

#### TIPOS PENALES PARA LA PROTECCION DE MENORES DE EDAD

Artículo 13.- Contacto de personas menores de edad a través de tecnologías de la información y la comunicación con fines sexuales

Conducta: Quien a través de tecnologías de la información y la comunicación, contacte con una persona menor de edad con el fin de cometer cualquiera de los delitos descritos en el título correspondiente a los delitos sexuales del Código Penal, o de obtener fotos o videos de la persona menor de edad en actividades sexuales explícitas o mostrando sus partes genitales o desnudo.

Agravantes: a) cuando el contacto se realice mediante coacción, intimidación, amenaza, engaño o seducción, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. b) Si con el fin de cometer este delito, el autor se hace pasar por una persona menor de edad para ganar la confianza de la víctima.

#### Artículo 14.- Pornografía virtual

Conducta: quien fabrique, produzca, reproduzca, comercialice, difunda o exhiba material pornográfico en el que no habiendo sido utilizados directamente personas menores de edad, emplee la imagen alterada o modificada, caricatura, dibujo o cualquier otra representación visual o la voz de una persona menor de edad, realizando actividades sexuales explícitas, o mostrando sus partes genitales o desnudos.

Artículo 15.- Publicidad de explotación sexual comercial de personas menores de edad asociada a viajes y turismo

Conducta: quien promueva o realice programas, campañas o anuncios publicitarios, a través de cualquier tecnología de la información y la comunicación, para proyectar al país a nivel nacional o internacional como un destino turístico accesible para la explotación sexual comercial en perjuicio de personas menores de edad.

#### Artículo 16.- Explotación sexual de personas menores de edad asociada a viajes y turismo

Conducta: a quien organice, dirija, gestione o facilite a través de cualquier tecnología de la información y la comunicación, viajes al territorio nacional o dentro de este, con el fin de cometer el mismo o un tercero, cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de edad, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos.

Agravante: En caso que la víctima sea menor de trece años de edad.

#### Artículo 17.- Ciberacoso entre personas menores de edad

Conducta: la persona menor de edad que amenace, hostigue, agrede o ultraje a otra persona menor de edad, a través de cualquier tecnología de la información y la comunicación. Al igual que la persona menor de edad que crea un sitio específico o formula mensajes a través de una tecnología de la información y la comunicación, dirigidos a motivar a terceros a que realicen las actividades anteriormente descritas.

El juez considerará al momento de determinar la pena si producto de las conductas anteriormente establecidas, se causan daños para la vida, integridad física o psíquica de la víctima.

#### Artículo 18.- Incitación a personas menores de edad a participar en juegos o actividades perjudiciales para la vida, la integridad física o psíquica

Conducta: Quien incite, por medio de cualquier tecnología de la información y la comunicación, a una persona menor de edad a realizar juegos o actividades violentas o de carácter sexual, que pongan en peligro su vida o su integridad física o psíquica

Agravantes: a) si la persona menor de edad sufre lesiones de cualquier naturaleza como producto de la incitación. b) Si producto de la incitación la persona menor de edad muere.

#### Artículo 19.- Ciberacoso a persona menor de edad

Conducta: Quien persiga, aceche o espíe a una persona menor de edad en perjuicio de su intimidad, a través de cualquier tecnología de la información y la comunicación.

MSc. CARLOS H. GÓNGORA FUENTES

Diputado

Asamblea Legislativa de Costa Rica