ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

LEY PARA COMBATIR LA CIBERDELINCUENCIA.

ERWEN MASÍS CASTRO
DIPUTADO

EXPEDIENTE N.º _____

PROYECTO DE LEY

LEY PARA COMBATIR LA CIBERDELINCUENCIA

Expediente N.º _____

ASAMBLEA LEGISTATIVA:

Este proyecto de ley nace debido a la necesidad de fortalecer nuestro ordenamiento jurídico en la lucha contra la ciberdelincuencia y con el fin de cumplir con los compromisos adquiridos por nuestro país a raíz de la ratificación del Convenio Europeo sobre Ciberdelincuencia.

El precedente nacional sobre una reforma al código penal sobre delitos informáticos estuvo impregnado de denuncias sobre posibles mordazas contra la prensa, por lo cual es importante que este proyecto que sanciona conductas en el ciberespacio tenga como prioridad proteger la libertad de expresión, al mismo tiempo que nos protege de flagelos cibernéticos que pueden desestabilizar nuestra democracia.

El cibercrimen cada vez afecta más usuarios, las investigaciones son complejas, nuestras autoridades no se encuentran preparadas, el ordenamiento jurídico costarricense no está preparado para investigaciones criminales digitales transfronterizas y las víctimas en algunas ocasiones se dan cuenta del ataque cuando ya es demasiado tarde.

De acuerdo con McAfee el cibercrimen tiene un costo anual de 600 billones de dólares a nivel mundial y de acuerdo a un estudio de RiskIQ, cada minuto 1861 personas son víctimas del cibercrimen, lo que genera pérdidas de 1.3 millones de dólares cada minuto.

Riesgos en la utilización de las TIC

La utilización de medios digitales conlleva riesgos de seguridad sobre los cuales la mayoría de la población no tiene conciencia, dado que la enseñanza sobre ciberseguridad es inexistente en la educación primaria y secundaria a nivel nacional y aún deficiente o inexistente en la educación superior relacionadas con las Tecnologías de la Información y Comunicación (TIC), lo que hace que exista una mayor vulnerabilidad de los usuarios que suelen ser víctimas, inclusive ante ataques poco sofisticados.

La lucha contra la ciberdelincuencia inicia desde la educación, ya que todo usuario debe saber qué hacer para evitar ser víctima de un delito informático o reducir los riesgos; pero también debe conocer qué debe hacer y qué no, cuando se da cuenta que ha sido víctima de un delito cometido por medios informáticos.

Lo primero, con el fin de hacerle más difícil el trabajo a los ciberdelincuentes y la segunda con el fin de reducir la impunidad. Muchas víctimas de delitos informáticos borran o manipulan evidencia digital por desconocimiento y terminan facilitándole al delincuente salir impune.

A continuación, se analizarán las amenazas predominantes en la utilización de las TIC.

El Phishing

Los ciberdelincuentes utilizan el engaño para poder tener acceso a datos personales de carácter confidencial o de acceso restringido con el objetivo final de atacar un sistema informático con información privilegiada obtenida, como lo puede ser una contraseña o datos del sistema que le permitan saber cómo atacarlo. Lo anterior se conoce como ingeniería social.

El ‘phishing’ lo podemos definir como un abuso informático “generalmente cometido a través del envío masivo de correo electrónico o SMS, suplantando la identidad de terceros mediante el uso de ingeniería social, con el fin de hacerse con información confidencial del usuario o instalar otro tipo de *malware”.*

Los usuarios suelen carecer de cultura de protección de datos personales, por lo que ante consultas por teléfono o correo electrónico, donde les requieren datos de carácter personal, confidencial o financiero, y los brindan en cantidades importantes, lo que le facilita el trabajo a los delincuentes. Si existiera mayor cultura digital y las personas se acostumbraran a no entregar datos personales por vías no presenciales, la mayoría de los delitos donde se utiliza el phishing como parte de los actos preparatorios del delitos no tendrían éxito.

En la estafa informática, el phishing se encuentra en el *iter criminis y* el delincuente busca obtener información como contraseñas y/o datos del segundo factor de autenticación que le permitan suplantarle la identidad a la víctima para realizar transferencias ilegítimas de fondos. Tomando en cuenta que los sistemas informáticos bancarios suelen ser difíciles de vulnerar, si las personas aprendieran a protegerse de ataques de ingenieria social, como el *phishing*, se podría reducir de forma significativa este tipo de delito.

Desde nuestro Código Penal se puede sancionar el ‘phishing’, a través de las siguientes conductas penales:

Suplantación de identidad: con pena de 1 a 3 años cuando la suplantación de una marca, persona física o jurídica se da a través de cualquier red social, sitio de Internet, medio electrónico o tecnológico de información.

Suplantación de Páginas electrónicas: con pena de 1 a 3 años cuando se suplanta un sitio legítimo de Internet en perjuicio de un tercero. Y la pena se agrava de 2 a 4 años, si a raíz de la suplantación se captan datos confidenciales, lo que es el 'phishing'.

En el presente proyecto de ley, también se sancionará la ingeniería social, siempre que siempre que no constituya delito con una pena superior.

Malware

En el año 2010 un artículo de la Revista Wired "The Web is dead, long live the internet" causó mucho revuelo ya que indicaba que la Web se encontraba muerta y que lo que seguía era un mundo de aplicaciones. Ocho años después podemos indicar que la visión de dicho artículo apuntaba al lugar correcto, ya que ahora las personas dependen de diferentes aplicaciones para distintas funciones, por lo que se han acostumbrado a instalar de forma continua aplicaciones para distintas acciones. Lo que ha llevado a los delincuentes a buscar instalar sus aplicaciones en los dispositivos de las víctimas, lo cual a diferencia de otros ataques, pone a las víctimas en constante peligro debido a las múltiples funciones que puede contener un 'malware'.

Los programas informáticos maliciosos son aquellos que atentan contra el titular del sistema informático y sus fines son tan diversos como lo son las actividades delictivas.

De acuerdo a Kaspersky, el 29.4% de los usuarios de computadoras fueron objeto de un ataque utilizando la web como medio de ataque en el año 2017.

La lucha contra el malware requiere de la ayuda de los desarrolladores de los sistemas operativos que utilizan miles de usuarios, ya que los ciberdelincuentes suelen aprovecharse de errores de programación o vulnerabilidades con el fin de obtener un beneficio.

Una de las formas de protegerse de este tipo de ataque es a través de la constante actualización de los sistemas, por lo que los usuarios dependen de la rápida corrección por parte de las empresas desarrolladores quienes a su vez dependen de la celeridad con que los usuarios instalen los parches de seguridad. Lo que nos deja claro que es una lucha que sólo puede librarse de forma coordinada y en conjunto.

El malware también puede propagarse a través de la utilización de sitios web atacantes, que son aquellos que intentan explotar vulnerabilidades de los navegadores de los usuarios con el fin de obtener privilegios sobre el sistema, con lo que podrían realizar, entre otras cosas, la instalación de un programa malicioso.

El ransomware “es software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados”. Es una de las amenazas más fuertes en este momento, en el año 2017, de acuerdo a Kaspersky, más de 939.722 usuarios únicos de Kaspersky Security Network fueron atacados, incluyendo más de doscientos cuarenta mil usuarios corporativos.

Sin embargo, para el año 2018 los programas informáticos maliciosos de minería oculta están superando al *ransomware* como la principal amenaza:

“El aumento en la cantidad de ataques con malwares mineros casi duplica las cifras registradas en 2016, que superan los 1,87 millones, pues Kaspersky Lab estima que se produjeron 2,7 millones de ataques con minería maliciosa a computadores tan solo en 2017.”

Por otro lado, el cibercrimen no es un área exclusiva del crimen organizado y en el caso del *malware* también es utilizado por parte de personas celosas con el fin de mantener control sobre su pareja sentimental, lo que nos aleja del cibercrimen organizado y nos lleva al cibercrimen que se realiza en el hogar.

Desde nuestro Código Penal se puede sancionar diferentes conductas relacionadas con la instalación o propagación de programas informáticos maliciosos en el artículo 232 del Código penal, cuya redacción actual es la siguiente:

> "Será sancionado con prisión de uno a seis años 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.

La pena será de tres a nueve años de prisión 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."

En el presente proyecto se incluye el verbo rector "ejecutar" en los casos donde un delincuente engañe a una persona para que ejecture un código malicioso dentro de su sistema informático, a pesar de que sea un programa que "corra" únicamente a nivel de navegador, pero que pueda resultar perjudicial para la víctima.

Suplantación de identidad

Los cibercriminales crean perfiles de las personas a través de la recolección de información personal que se encuentra en fuentes disponibles al público o a través de la adquisición en el mercado, regularmente en la internet oscura (Dark Web o Deep Web), donde se acepta como método de pago las criptomonedas, que le permiten al delincuente ocultar su identidad.

Con los datos personales de las víctimas les pueden suplantar la identidad por medios electrónicos con fines distintos, desde el acoso cibernético hasta la estafa informática.

El robo de datos personales también puede utilizarse para crear un perfil falso en redes sociales para engañar menores de edad y así seducirlos, obtener documentos de índole íntima y/o buscar un encuentro físico con el menor, con el fin de abusarle o violarle.

A través de la utilización de una cantidad importante de datos personales de una persona se puede lograr realizar montajes en video o audio de personas con las que se logra un montaje creíble para terceros que quien se encuentra realizando acción en video es la persona que está sufriendo, lo que se conoce como *deepfakes* y que algunos expertos advierten que este abuso informático podría ayudar en la manipulación de las próximas elecciones de los Estados Unidos:

«Un reciente estudio titulado 'Inteligencia artificial y seguridad internacional' indica cómo los DeepFakes, una técnica de inteligencia artificial (IA) utilizada para crear imágenes o videos falsos de gente real, representa una de las mayores amenazas de esta tecnología.

Según la explicación de los autores del estudio, los sistemas de inteligencia artificial *"son capaces de generar grabaciones de voces sintéticas con sonido realista"* de cualquier individuo del cual exista suficiente registro para entrenar a la inteligencia artificial.

Los videos generados por DeepFakes son normalmente fáciles de detectar por cualquier persona, no obstante, el avance de esta tecnología va tan rápido que en menos de cinco años podría llegar a engañar a cualquier ojo u oído sin entrenamiento para detectar estas falsedades»..

Para luchar contra flagelos como el citado supra lo más importante es que las personas cuiden sus datos personales, para no darles material a los delincuentes para que puedan realizar estos montajes tan creíbles y por lo tanto dañinos.

Al mismo tiempo, la suplantación de identidad debe extenderse a aplicaciones informáticas, donde una persona puede valerse de la reputación de una ‘app’ en una tienda de aplicaciones para así capturar una cantidad de personas que buscan la misma y en algún momento atentar contra estos.

En el presente proyecto de ley se amplía la protección a marcas, más allá de las comerciales, como lo puede ser el caso de marcas institucionales.

Noticias falsas

En los últimos años han surgido acusaciones serias de manipulación del electorado con noticias falsas, lo que ha dejado expuesto a las plataformas tecnológicas por el poco esfuerzo que han puesto en el combate de los llamados *fake news*, debido a que esta técnica ha podido ser utilizada por gobiernos extranjeros para incidir en un resultado electoral.

El caso más emblemático es el de las elecciones de los Estados Unidos en el año 2016, donde se piensa que existió una manipulación del gobierno ruso, lo que le ayudó a Donald Trump a llegar al poder, como lo relata la BBC Mundo:

“Trece ciudadanos y tres compañías rusas fueron acusadas formalmente este viernes por el Departamento de Justicia de Estados Unidos de interferir en las elecciones presidenciales de 2016. Se les acusa de "violar las leyes criminales para interferir en los comicios de EE.UU. y los procesos políticos", señaló la oficina del fiscal especial Robert Mueller, quien investiga la presunta interferencia rusa en la campaña.

Entre sus operaciones, figuran la comunicación de "información despectiva sobre Hillary Clinton, denigrar a otros candidatos como Ted Cruz y Marco Rubio, y apoyar a Bernie Sanders y al entonces candidato Donald Trump".

Reciéntemente también salieron a relucir las estrategias utilizadas para difundir las noticias falsas de acuerdo a los intereses de sus objetivos, a través del tratamiento ilegal de datos personales de estos. La controversiales acciones consistieron en lo siguiente:

“Un modelo de psicología y un algoritmo de extraordinaria precisión sirvieron a Cambridge Analytica para analizar los perfiles de millones de usuarios de Facebook e intentar influenciar en sus votos.

Alexander Nix, exjefe de la compañía británica, dijo que había logrado hacer un perfil de personalidad de "cada adulto en Estados Unidos" y de esta forma había conseguido influenciar en el resultado de las elecciones que convirtieron a Donald Trump en presidente de Estados Unidos.

El modelo de los cinco grandes rasgos de personalidad, que se utiliza en psicología, le sirvió de base.”.

La responsabilidad ha recaído sobre la plataforma tecnológica quien para la fecha de los hechos permitía que con el consentimiento de un usuario de la red social se recopilaran datos personales de sus amigos, lo cual es una flagrante vulnerabilidad y violación de las diferentes leyes de protección de datos personales donde Facebook tiene presencia.

Al mismo tiempo, Facebook nunca se cercioró que las empresas que creaban aplicaciones que capturaban datos personales, a través de su plataforma, cumplían con los términos de servicio de la red social, por lo que esto fue aprovechado para realizar actos de captación de datos personales a gran escala.

El sancionar la difusión de noticias falsas puede ser peligroso en un país con una democracia vulnerable y aún en un país como Costa Rica debe realizarse con mucho cuidado, con el fin de asegurarse que una regulación no venga a darle poder

a grupos de presión para perseguir penalmente a periodistas debido a errores propios de su profesión.

En este sentido, el proyecto viene a brindar herramientas para luchar contra este flagelo sin poner en peligro la libertad de prensa o expresión.

También es cierto que no se deben generar sanciones penales en contra de proveedores de servicios electrónicos por el material que otros publican en sus plataformas, pero sí se debe tener los medios para cooperar con estas empresas de forma eficaz, con el fin de poder perseguir penalmente a quienes **fabriquen y difundan** noticias falsas.

Acoso Cibernético.

La ubicuidad de la tecnología en la sociedad moderna y la dependencia tecnológica que va generando en los ciudadanos hace que estas vayan formando parte de nuestra realidad, por lo que todo lo que suceda en el mundo virtual tenga un efecto importante sobre las personas.

En el caso del acoso por medios electrónicos puede generar un impacto psicológico en las víctimas bastante fuerte, debido a que dependiendo de los recursos tecnológicos con los que cuente el acosador, así hará notar su presencia alrededor de la víctima, quien confundirá el acoso digital con peligro en el mundo físico.

El acoso digital puede realizarse a través de acciones que encuadran en un tipo penal informático, por lo que pueden perseguirse penalmente, pero también pueden realizarse a través de abusos informáticos que no se encuentran tipificados en el Código Penal, por lo cual las víctimas pueden sentirse desprotegidas cuando se presentan este tipo de acciones.

En el caso de España, la Ley Orgánica 1/2015 reformó al Código Penal e introdujo el acoso incesante a una persona en el artículo 172 ter que reza lo siguiente:

«1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1.ª La vigile, la persiga o busque su cercanía física.

2.ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.

3.ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.

2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.

3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.

4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.

Sobre este tipo penal el autor CÁMARA Sergio, indica “Las conductas de stalking afectan el proceso de formación de la voluntad de la víctima en tanto que la sensación de temor e intranquilidad o angustia que produce el repetido acechamiento por parte del acosador le lleva a cambiar sus hábitos, sus horarios, sus lugares de paso, sus números de teléfono, cuentas de correo electrónico e incluso de lugar de residencia y trabajo. Se protege asimismo el bien jurídico de la seguridad. Esto es el derecho al sosiego y a la tranquilidad personal. No obstante solo adquirirán relevancia las conductas que limiten la libertad de obrar del sujeto pasivo, sin que el mero sentimiento de temor o molestia sea punible. Por último hemos de advertir que, aunque el bien jurídico principalmente afectado por el *stalking* sea el de la libertad, también pueden verse afectados otros bienes jurídicos como el honor, la integridad moral o la intimidad, en función de los actos en que se concrete el acoso”.

En opinión de las autoras DAVARA Laura y DAVARA Elena, este artículo viene a dar cabida “a todas aquellas actuaciones -molestas y altamente dañinas- que, sin duda, causan un menoscabo en la víctima, tanto a lo que respecta a su propia libertad como a su dignidad y seguridad. Y es que, tal y como establece el propio artículo, las acciones llevadas a cabo con objeto de acosar incesantemente llevan aparejada la alteración grave del desarrollo de la vida cotidiana”.

En la resolución 416/2017 de la Audiencia Provincial de la Coruña el tribunal ahonda sobre este tipo penal:

«Ya respecto al tipo penal explica el Tribunal Supremo que "Con la introducción del art. 172 ter CP nuestro ordenamiento penal se incorpora al creciente listado de países que cuentan con un delito con esa morfología. La primera ley antistalking se aprobó en California en 1990. La iniciativa se fue extendiendo por los demás estados confederados hasta 1996 año en que ya existía legislación específica no solo en todos ellos, sino también un delito federal. Canadá, Australia, Reino Unido, Nueva Zelanda siguieron esa estela a la que se fueron sumando países de tradición jurídica continental: Alemania (Nachstellung), Austria (behrrliche Verfolgung), Países Bajos, Dinamarca, Bélgica o Italia (atti persecutori). En unos casos se pone más el acento en el bien jurídico seguridad, exigiendo en la conducta una aptitud para causar temor; en otros, como el nuestro, se enfatiza la afectación de la libertad que queda maltratada por esa obsesiva actividad intrusa que puede llegar a condicionar costumbres o hábitos, como única forma de sacudirse la sensación de atosigamiento."

En los intentos de conceptualizar el fenómeno del *stalking* desde perspectivas extrajurídicas -sociológica, psicológica o psiquiátrica- se manejan habitualmente, con unos u otros matices, una serie de notas: persecución repetitiva e intrusiva; obsesión, al menos aparente; aptitud para generar temor o desasosiego o condicionar la vida de la víctima; oposición de ésta... Pues bien, es muy frecuente en esos ámbitos exigir también un cierto lapso temporal. Algunos reputados especialistas han fijado como guía orientativa, un periodo no inferior a un mes (además de, al menos, diez intrusiones). Otros llegan a hablar de seis meses.

Esos acercamientos metajurídicos no condicionan la interpretación de la concreta formulación típica que elija el legislador. Se trata de estudios desarrollados en otros ámbitos de conocimiento dirigidos a favorecer el análisis científico y sociológico del fenómeno y su comprensión clínica. Pero tampoco son orientaciones totalmente descartables: ayudan en la tarea de

esclarecer la conducta que el legislador quiere reprimir penalmente y desentrañar lo que exige el tipo penal, de forma explícita o implícita.

No es sensato ni pertinente ni establecer un mínimo número de actos intrusivos como se ensaya en algunas definiciones, ni fijar un mínimo lapso temporal. Pero sí podemos destacar que el dato de una vocación de cierta perdurabilidad es exigencia del delito descrito en el art. 172 ter CP , pues solo desde ahí se puede dar el salto a esa incidencia en la vida cotidiana. No se aprecia en el supuesto analizado esa relevancia temporal -no hay visos nítidos de continuidad-, ni se describe en el hecho probado una concreta repercusión en los hábitos de vida de la recurrente como exige el tipo penal.»

Como puede verse la fórmula utilizada por el Código Penal español es limitada en el sentido que excluye acciones que podrían afectar el bien jurídico a pesar de que la misma no se dé de una forma reiterativa pero con la suficiente fuerza para afectar el bien jurídico penalmente.

Toda reforma sobre delitos informáticos debe proteger la libertad de expresión no menoscabarla.

Como se ha analizado, existen diferentes acciones que representan riesgos para los usuarios que deben ser reguladas, pero que si la tarea se le da a un legislador que responde a sus propios intereses, o a los de terceros, puede poner en riesgo la libertad de expresión, al sancionar acciones que pueden ser realizadas por activistas, periodistas o investigadores, pero que son incorporadas como delitos en una reforma al código penal.

Por lo anterior, toda legislación que busque regular las TIC debería ser consultada con la sociedad civil, especialistas locales e internacionales, organismos internacionales especializados en la materia, colegios profesionales afines y demás partes interesadas, con el fin de que puedan pronunciarse sobre la propuesta.

La libertad de expresión es el pilar de toda sociedad moderna y el ejercicio de la misma a través de medios tecnológicos se ha convertido en la forma predominante y la más efectiva, por lo que cada vez que se pretende regular las TIC existe mucha preocupación de que se busquen formas de censurar a la población.

Sobre este proyecto de ley.

El código penal costarricense es bastante moderno en cuanto a las conductas que sanciona y le permite a las autoridades poder perseguir penalmente las actividades cibercriminales que se dan en contra de habitantes de nuestro territorio.

El nuevo proyecto de ley no solo viene a dar solución a errores que se cometieron en las reformas 9048 y 9135, sino que también viene a incluir nuevos tipos penales, que ayudarán a reducir la impunidad en la comisión de este nuevo tipo de conductas abusivas que en el presente no pueden ser sancionadas.

Uno de los principales problemas que se tiene al analizar los tipos penales informáticos tienen que ver con su correcta interpretación, más cuando sancionan complejas conductas delictivas y se utiliza lenguaje informático que debe ser interpretado de forma correcta. Este proyecto de ley, contiene un importante apartado de definiciones que servirán tanto para una mejor comprensión sobre los tipos penales informáticos, sino que también va a permitir un mejor estudio de la academia sobre esta materia.

Esta nueva propuesta de proyecto viene a sancionar las siguientes conductas delictivas:

Acoso cibernético: con una fuerte influencia del Código penal español, pero fortalecida con las conductas más comunes que enfrentan las víctimas de esta clase de delitos y las que se espera que se utilicen en un futuro.

Captación de actos o partes íntimas: la omnipresencia de las nuevas tecnologías de la información y comunicación le han facilitado a los delincuentes poder grabar a personas en sus momentos más íntimos, pasar inadvertidos y luego difundir dichos contenidos en internet con gran afectación para los afectados.

Difusión o tráfico de contraseñas o vulnerabilidades: las contraseñas son la puerta de ingreso a muchos sistemas informáticos, de la misma forma como una vulnerabilidad puede permitir que un delincuente acceda a un sistema informático sin mayor problema, por lo que el tráfico de estas debe ser sancionado por ley.

Ingeniería social: Con el fin de poder perseguir a los ciberdelincuentes, en la etapa de recolección de información confidencial que puede ser utilizada para cometer otros delitos informáticos y siempre que no constituya delito con una pena superior, se impondrá pena de prisión de seis meses a dos años a quien, mediante engaño, capture u obtenga datos personales o información confidencial apta para la comisión de un delito informático.

Difusión de noticias falsas: la utilización de perfiles falsos, páginas de Facebook y sitios web especializados en difundir noticias falsas con el fin de manipular el electorado es una tendencia mundial y debe sancionarse penalmente si este acto es realizado con el fin de manipular la decisión de los ciudadanos con la utilización de hechos flagrantemente falsos. En este tipo penal se ha sido muy cuidadoso, para dejar claro que no podría utilizarse para perseguir comunicadores en el ejercicio de su profesión.

Ciberacoso sexual: las propuestas sexuales o envío de mensajes de contenido pornográfico de forma no solicitada, reiterada y fuera del marco de una comunicación recíproca de índole sexual o erótica a otra persona, con la quien no

tenga una relación de pareja o índole sexual, tendrá una pena de será reprimido con pena de treinta a cincuenta días multa.

Compras ilícitas mediantes tarjetas: a solicitud de la Fiscalía, se inclue este tipo penal que sancionará con penas de prisión de dos a cinco años a a quien ilícitamente adquiera bienes o servicios, a través del uso de una tarjeta de crédito o de débito no expedida en su favor, o mediante el uso de otro medio de pago electrónico; sin la autorización del titular.

Acceso ilícito: en cumplimiento de lo requerido por el Convenio Europeo sobre Ciberdelincuencia será sancionado con prisión de seis meses a un año de prisión a quien, evadiendo medidas de seguridad y con fines maliciosos, acceda a un sistema informático, sin la autorización del titular.

Abuso de dispositivos: en cumplimiento de lo requerido por el Convenio Europeo sobre Ciberdelincuencia, Se impondrá pena de prisión de uno a cinco años a quien distribuya, produzca, venda, compre, obtenga para su utilización o importe un dispositivo o programa informático diseñado o adaptado principalmente para la comisión de delitos informáticos.

Después de un análisis de las obligaciones que adquirió Costa Rica, con el Convenio Europeo sobre Ciberdelincuencia, podríamos ver que la falsificación informática no se encuentra contenida dentro del grupo de normas que se encuentran en este proyecto ley. Sin embargo, de acuerdo al principio de equivalencia funcional en los casos de falsedad ideológica, falsificación de documentos privados, falsificación de documentos públicos y auténticos, cumplen a cabalidad con lo contenido en el Convenio de Budapest.

Herramientas procesales

La mayoría de investigaciones sobre delitos informáticos, requieren de la cooperación con la empresa privada, extranjera o nacional, lo que si no se cuenta con protocolos de actuación y alianzas con la empresa privada, las investigaciones

pueden atrasarse o en el peor de los casos detenerse debido a obstáculos que pueden ser previstos.

El obstáculo más grande con el que cuenta un país como el costarricense, cuyos ciudadanos utilizan principalmente plataformas tecnológicas, cuyos servidores se encuentran principalmente en los Estados Unidos u otras naciones europeas, es que al encontrarse el responsable de la base de datos que contienen los datos que son necesarios para una investigación criminal digital, no existe forma de obligarlos a cooperar con nuestras autoridades. Sin embargo, muchas de las grandes empresas que utilizan los costarricenses ya cuentan con plataformas u protocolos de cooperación con las autoridades nacionales en la investigación de delitos que se dan en sus plataformas.

Es por esto, que este proyecto propone la creación de la Comisión Nacional de lucha contra la Ciberdelincuencia, que vendrá a convertirse en una plataforma de diálogo con la empresa nacional y extranjera con el fin de mejorar la cooperación en la investigación criminal. Al mismo tiempo, no se vienen a imponer sanciones a las empresas extranjeras que incumplan la normativa, debido a que el espíritu de la ley es que como primera fase se puedan lograr acuerdos, que tome como base la solidez de nuestra democracia y el espíritu de colaboración que ya han demostrado empresas como Microsoft, Google, Facebook y Apple para cooperar en investigaciones criminales donde existan garantías de respeto de los derechos fundamentales.

La Comisión Nacional de Lucha contra la Ciberdelincuencia estará encargada de:

- Crear y mantener actualizada la Estrategia Nacional de lucha contra la ciberdelincuencia.

- Elaborar un informe, que deberá ser publicado cada dos años, sobre la eficacia del Ordenamiento Jurídico costarricense en la lucha contra la ciberdelincuencia.

- Elaborar una lista de proveedores relevantes de servicios electrónicos, para lo cual deberá tomar en cuenta el impacto para la sociedad costarricense de los servicios informáticos y de telecomunicaciones y, cuando se encuentre disponible, la cantidad de usuarios costarricenses que usan dichos servicios.

- Sugerir protocolos de actuación para la investigación de delitos informáticos.

- Sugerir protocolos de cooperación en la investigación de delitos informáticos y computacionales con los operadores de telecomunicaciones nacionales y los proveedores esenciales de servicios electrónicos.

- Con base en estadísticas o datos judiciales, policiales o en general que sean de utilidad, provenientes de la cooperación con los proveedores de servicio en la investigación criminal, se realizará una calificación anual de los mismos, con el fin de identificar puntos de mejora.

En el artículo sexto de este proyecto de ley indica que todo proveedor de servicios electrónicos u operador de telecomunicaciones se encuentra obligado a:

1. Conservar y proteger la integridad de los datos electrónicos o similares relacionados con una acción delictiva, ante la solicitud del Ministerio Público o la Policía Judicial, de acuerdo a los artículos 286 inciso b) y 291 del Código

Procesal Penal, por un lapso de cuatro años o hasta su prescripción legal.

2. Cumplir con la entrega de información requerida por los Tribunales de Justicia, en un plazo máximo de 24 horas, dentro de la investigación de un delito informático donde se encuentre en peligro la vida, la salud o la integridad física de uno o varias personas.

3. Cumplir con la entrega de datos de abonado, de tráfico o de localización requeridos por los Tribunales de Justicia, en un plazo máximo de 48 horas, dentro de la investigación de un delito informático o vinculado con pornografía infantil.

4. Cumplir con la entrega de datos de tráfico, de localización o de abonado requeridos por por los Tribunales de Justicia, en un plazo máximo 7 días hábiles, dentro de la investigación de un delito cometido por vías informáticas.

5. Proteger la confidencialidad de los datos y de las acciones requeridas por las autoridades judiciales. La obligación de secreto funcional se extiende a empleados o funcionarios del proveedor u operador, así como a las empresas o personas que le brinden servicios, en concordancia con la obligación de confidencialidad señalada en el Código Procesal Penal.

Los datos de abonado, de localización o de tráfico, en el marco de una investigación penal judicial, podrán ser entregados ante solicitud del Ministerio Público o de la Policía Judicial, si el proveedor de servicios cuenta con el consentimiento de sus clientes, indicado en los términos del contrato de servicio o política de privacidad. En caso contrario, requerirá de autorización judicial. El proveedor podrá requerir que la entrega de la información sea autorizada por un juez penal, para cumplir con su legislación local.

Lo que se busca con esta norma procesal es, en una primera etapa, lograr que a través de la Comisión Nacional de lucha contra la Ciberdelincuencia es que todos los proveedores de servicios electrónicos costarricenses reformen sus políticas de privacidad con el fin de que sus clientes se encuentren informados que en caso de una investigación criminal sus datos podrán ser compartidos con el Ministerio Público o Policía Judicial. Al mismo tiempo que esto viene a permitir, que en el caso de proveedores extranjeros, en respeto a nuestra legislación interna puedan cooperar de una forma más ágil con el Ministerio Público o Policía Judicial, lo que traería mayor celeridad a los procesos de cooperación internacional cuando se trate de datos de tráfico o de abonado, más no contenido donde para poder tener acceso a los mismos, en respeto de nuestra constitución deberá ser a través de una orden judicial.

Transparencia público-privada.

Todo proveedor u operador costarricense de relevancia en servicios electrónicos o de telecomunicaciones deberá hacer un reporte anual de transparencia con respecto a la entrega de información de sus clientes a las autoridades judiciales y clasificada por el tipo de investigación de delitos para el cual fue solicitada.

Empresas estadunidenses han sido líderes en la creación de reportes de transparencia, dirigido a saber de qué forma se está cooperando con las autoridades y de esta forma no solo brindar estadísticas que podrán ser utilizadas para la discusión nacional sobre esta materia, sino que traerán tranquilidad a los costarricenses para saber de qué forma se está compartiendo su información dentro del marco de una investigación criminal.

Remoción de contenido.

En casos de acoso cibernético, pornografía infantil es necesario que las autoridades avancen con procesos de remoción de contenido, en respeto de la libertad de expresión y prensa.

Por lo que de acuerdo al artículo sétimo del proyecto de ley:

> **ARTÍCULO 7. Remoción de contenido en casos de Acoso Cibernético o Pornografía infantil.**
>
> Dentro de un máximo de 24 horas posteriores a la interposición de la denuncia por los delitos de acoso cibernético o pornografía infantil, a solicitud del Ministerio Público, **un juez deberá resolver la solicitud de remoción del contenido publicado o difundido en la ejecución del delito informático**, dirigida al **proveedor de servicios electrónicos o al ofensor en cualquier medio que tenga bajo su control.**
>
> El juez deberá valorar que, a través de esta medida, no se pueda generar una afectación irreparable a la libertad de expresión y/o al derecho de acceso a la información.
>
> El juez podrá conceder la remoción parcial del contenido, como puede ser la eliminación de datos específicos de un documento o contenido, si considera que con esto se logra un balance entre la protección de los derechos de la víctima y la libertad de expresión.

Como puede verse, el juez podrá solicitarle de forma directa al ofensor o al proveedor de servicios que dicho contenido deba retirar el contenido, siempre y cuando esto no genere una afectación irreparable a la libertad de expresión, por lo que salvo que sea una ofensa flagrante, el juez podría solicitar la remoción del

contenido parcial, como podría ser una imagen de contenido sexual en alguna publicación en un sitio web.

Definitivamente el país necesita ampliar el marco regulatorio vigente y emprender una serie de reformas legales para empezar a combatir de forma más eficiente la criminalidad informática, que tan negativamente impacta en nuestra sociedad.

Por las razones anteriormente expuestas es que se somete a la consideración de la Asamblea Legislativa el presente proyecto de ley.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:

LEY PARA COMBATIR LA CRIMINALIDAD INFORMÁTICA

ARTÍCULO 1.- Definiciones.
Para los efectos de la presente ley y del Código Penal, se define lo siguiente:

1. **Activo digital:** Cualquier recurso u objeto que existe de forma electrónica y que alguien puede utilizar, poseer o administrar, por lo que tiene asociado un derecho. Como por ejemplo, una página de facebook. cuenta de twitter, cuenta de youtube, cuenta de administración de una plataforma de gestión de correos electrónicos, una cuenta de correo electrónico, entre otros.
2. **Acto íntimo:** Todo acto sexual realizado en un espacio privado y/o con expectativa de intimidad.
3. **Aplicación informática**: programas para dispositivos móviles u ordenadores que permiten al usuario realizar distintas acciones de carácter secundario y no necesarias para el funcionamiento básico del sistema operativo.
4. **Base de datos electrónica:** Sistema lógico y automatizado, compuesto por un conjunto almacenado, compilado y ordenado de registros que almacenan datos de cualquier índole y para un fin determinado, creado mediante un lenguaje de programación apropiado e instalable en una plataforma de computadores, que brinda información como respuesta del sistema.
5. **Cibercrimen**: Actividad delictiva cuyas conductas tienen como eje central la utilización de medios electrónicos, con el objetivo de vulnerar bienes jurídicos tutelados penalmente. Ejemplo de ello son las ciberestafas, estafas informáticas, suplantación de identidad, violación de comunicaciones, de datos personales, sabotaje, daños, hurto, todo ello de carácter informático o electrónico, entre otros.
6. **Ciberestafa**: Estafa tradicional que se comete por medios informáticos. Ejemplo de ello es la “estafa nigeriana” y similares.
7. **Captura:** Apoderarse, tomar o captar datos, sonidos, charlas, conversaciones, imágenes, vídeos o contenido audiovisual, usualmente sin el conocimiento o consentimiento de la persona.
8. **Datos de tráfico:** cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático o de telecomunicaciones, generados por un equipo tecnológico como elemento de la cadena de comunicación, que indiquen el origen, destino, ubicación, ruta, hora, fecha, tamaño o duración de la comunicación o el tipo de servicio subyacente.

9. **Datos de localización:** cualesquiera datos informáticos relativos a la localización geográfica y temporal de un usuario o de un equipo de comunicación por medio de un servicio de telecomunicaciones.
10. **Datos informáticos:** cualquier representación electrónica de hechos, información o conceptos ordenados de forma tal que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.
11. **Datos de abonado**: toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, que permitan determinar: 1. el tipo de servicio de comunicaciones utilizado 2. La identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios. 3. Cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

12. **Datos personales sensibles**: información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial, opiniones políticas, condición de salud, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros.
13. **Delito informático**: toda aquella acción delictiva de carácter informático o electrónico dirigida a vulnerar la confidencialidad, integridad o disponibilidad de los sistemas o datos informáticos, o contra la autodeterminación informativa y/o la identidad en medios electrónicos.
14. **Delito Computacional**: Delitos tradicionales cometidos mediante la utilización de nuevas tecnologías, medios informáticos, electrónicos, telemáticos, ópticos o magnéticos.

15. **Documento**: Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio físico, electrónico, telemático o informático, tales como archivos de audio, video o imágenes, indicadas en el artículo 1 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones No.7425 de 1994 o el artículo 6 bis de la Ley Orgánica del Poder Judicial, entre otros.
16. **Fabricación de noticias falsas:** toda creación de uno o más hechos falsos, a través de la utilización de medios creados con el fin de engañar o inducir en error al público en general, tales como sitios Web, páginas electrónicas, cuentas personales en medios digitales, imágenes, audios o videos.
17. **Invitación pública**: cualquier invitación realizada por medios físicos o electrónicos, dirigida al público general o a un grupo de personas. **Instalación de programas:** Es el proceso de transferencia o copia de los archivos o código de un programa, al sistema informático, en preparación para su ejecución, que puede requerir, o no, configuraciones adicionales en el sistema.

18. **Infraestructura crítica**: Se refiere a las instalaciones, redes, servicios o equipos físicos o de tecnologías de la información y comunicación cuya interrupción o destrucción tendría impacto en la vida, salud, seguridad o bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas, cuyo funcionamiento óptimo es indispensable por falta de soluciones alternativas ante su eventual ausencia o, existiendo, tengan un costo muy elevado, por lo que su desmejoramiento o destrucción tendría un impacto considerable sobre algún grupo humano.
19. **Medio social:** Plataforma de comunicación en línea o en redes de telecomunicación abierta donde el contenido es creado y puesto a disposición por los propios usuarios. Este tipo de medio facilita la edición, la publicación y el intercambio de información. Ejemplos de medios sociales son las redes sociales o de información, plataformas de vídeo, aplicaciones de

mensajería electrónica, tales como Facebook, WhatsApp, Wikipedia, Twitter y similares.

20. **Noticia falsa:** Hecho falso, incompleto o inexacto, divulgado con conocimiento de su falsedad y con intención de engañar o hacer incurrir en error al destinatario, diferente a la parodia o al ejercicio periodístico.
21. **Pornografía infantil:** 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. Incluye toda representación de las partes genitales de una persona menor de edad con fines sexuales.
22. **Programa de cómputo:** conjunto de instrucciones expresadas mediante palabras, códigos, gráficos, diseño o en cualquier otra forma que, al ser incorporados en un dispositivo de lectura automatizada, es capaz de hacer que una computadora -un aparato electrónico o similar capaz de elaborar informaciones- ejecute determinada tarea u obtenga determinado resultado.

23. **Programa informático malicioso:** es un código o programa informático diseñado con fines ilícitos que atenta contra la integridad de los bienes informáticos, datos personales, financieros o actividades cotidianas del titular del sistema informático o de sus legítimos usuarios.
24. **Proveedor de servicios electrónicos:** toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático. A su vez, se considerará como tal a cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio.
25. **Red de ordenadores zombi:** Conjunto de computadoras controladas por otro ordenador de forma remota, con el fin de cometer abusos o delitos informáticos.
26. **Sistema informático**: todo dispositivo, tanto aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o

varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

27. **Sistemas informáticos de salud:** sistemas informáticos que controlan la operación de un dispositivo médico, o bien, aplicaciones que tienen como fin tratar datos personales sensibles de índole médica.
28. **Sitios de Internet legítimos:** sitios o páginas Web diseñados para el conocimiento o difusión de ideas, opiniones, entretenimiento, redes sociales, publicidad, noticias, bancarias, financieras, de Gobierno, servicios de todo tipo o, en general, cualquier otra forma de comercio electrónico, libertad de comercio o de expresión, etc., de carácter lícito y apegado a las normas jurídicas.
29. **Sitios de Internet atacantes:** sitios o páginas Web que ejecutan acciones en perjuicio de quienes las visitan, como la promoción de instalación de programas maliciosos, la explotación de vulnerabilidades de un programa navegador de Internet, de un sistema informático o de sus componentes, entre otras actividades ilícitas o ilegítimas.
30. **Soporte de almacenamiento:** Espacio diseñado al efecto donde se registra o guarda información, el cual puede ser de carácter físico, electrónico, magnético, óptico, genético o de cualquier clase que sea capaz de contener y mantener información. Ejemplo de ello son los discos duros, discos ópticos compactos de todo tipo, unidades de memoria flash, etc. y todos aquellos que, con ese fin, ofrezcan las nuevas tecnologías.
31. **Vulnerabilidad**: Fallo o deficiencia de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas, tanto de manera remota como inmediata, sobre un sistema informático.

ARTÍCULO 2. Difusión de información de interés público.

Para efectos de aplicación de la presente ley y los tipos penales informáticos contenidos en el Código Penal, no constituirá delito:

1. La publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

2. La copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley.

3. La publicación reiterada e insistente de reportajes o denuncias de interés público.

ARTÍCULO 3. Investigación criminal.

Para efectos de aplicación de la presente ley y los tipos penales informáticos contenidos en el Código Penal, no constituirá delito:

1. La ingeniería social por parte de las autoridades en el marco de una investigación criminal.
2. La comisión de una acción típica contenida en un tipo penal informático presente en el Código Penal o esta ley, si la misma ha sido realizada con la autorización de un juez penal.
3. La captación de datos de ubicación geográfica obtenidos en el desarrollo de los actos y procedimientos de carácter policial o judicial llevados a cabo en el marco o en el transcurso de investigaciones de naturaleza informática, electrónica o telemática, mediante el uso necesario de herramientas electrónicas, programas o aplicaciones informáticas, aparatos electrónicos o sistemas de telecomunicaciones.

ARTÍCULO 4. Comisión Nacional de Lucha contra la Ciberdelincuencia.

Se crea la Comisión Nacional de Lucha contra la Ciberdelincuencia, que estará conformada por:

1. Un(a) representante de la Sala Tercera Penal de la Corte Suprema de Justicia del Poder Judicial, que deberá ser Magistrado(a) de dicha Sala, designado por ésta.
2. El (la) director(a) del Organismo de Investigación Judicial.
3. El(la) director(a) de la Sección de Delitos Informáticos del Organismo de Investigación Judicial.
4. Un(a) representante de la Fiscalía General de la República.
5. Un(a) representante de la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) del Poder Judicial.
6. Un(a) representante del Centro de Respuesta de Incidentes Informáticos - CSIRT-CR del Ministerio de Ciencia y Tecnología.
7. Un(a) representante de la Comisión de Derecho Informático del Colegio de Abogados y Abogadas de Costa Rica.

La Comisión Nacional de Lucha contra la Ciberdelincuencia estará encargada de:

- Crear y mantener actualizada la Estrategia Nacional de lucha contra la ciberdelincuencia.

- Elaborar un informe, que deberá ser publicado cada dos años, sobre la eficacia del Ordenamiento Jurídico costarricense en la lucha contra la ciberdelincuencia.

- Elaborar una lista de proveedores relevantes de servicios electrónicos, para lo cual deberá tomar en cuenta el impacto para la sociedad costarricense de los servicios informáticos y de telecomunicaciones y, cuando se encuentre disponible, la cantidad de

usuarios costarricenses que usan dichos servicios.

- Sugerir protocolos de actuación para la investigación de delitos informáticos.

- Sugerir protocolos de cooperación en la investigación de delitos informáticos y computacionales con los operadores de telecomunicaciones nacionales y los proveedores esenciales de servicios electrónicos.

- Con base en estadísticas o datos judiciales, policiales o en general que sean de utilidad, provenientes de la cooperación con los proveedores de servicio en la investigación criminal, se realizará una calificación anual de los mismos, con el fin de identificar puntos de mejora.

Los protocolos de actuación para la investigación de delitos informáticos y para la cooperación internacional serán enviados a la Fiscalía General para su valoración.

ARTÍCULO 5. Protocolos de cooperación en la investigación de delitos informáticos con proveedores extranjeros.

La Comisión Nacional de Lucha contra la Ciberdelincuencia convocará a representantes de los proveedores esenciales de servicios electrónicos, sean nacionales o extranjeros, con el fin de crear de forma conjunta protocolos de cooperación para la investigación de delitos informáticos o cualquier otro delito que

sea cometido con la ayuda de las nuevas tecnologías o donde exista evidencia digital en control del proveedor de servicio.

Deberá crearse un protocolo especial para cooperación en casos de urgencia, por estar en peligro las evidencias digitales, la vida, la salud o la integridad física de una o más personas.

ARTÍCULO 6.- Cooperación de los proveedores de servicios electrónicos en el marco de una investigación de delitos informáticos.

Todo proveedor de servicios electrónicos u operador de telecomunicaciones se encuentra obligado a:

1. Conservar y proteger la integridad de los datos electrónicos o similares relacionados con una acción delictiva, ante la solicitud del Ministerio Público o la Policía Judicial, de acuerdo a los artículos 286 inciso b) y 291 del Código Procesal Penal, por un lapso de cuatro años o hasta su prescripción legal.

2. Cumplir con la entrega de información requerida por los Tribunales de Justicia, en un plazo máximo de 24 horas, dentro de la investigación de un delito informático donde se encuentre en peligro la vida, la salud o la integridad física de uno o varias personas.

3. Cumplir con la entrega de datos de abonado, de tráfico o de localización requeridos por los Tribunales de Justicia, en un plazo

máximo de 48 horas, dentro de la investigación de un delito informático o vinculado con pornografía infantil.

4. Cumplir con la entrega de datos de tráfico, de localización o de abonado requeridos por por los Tribunales de Justicia, en un plazo máximo 7 días hábiles, dentro de la investigación de un delito cometido por vías informáticas.

5. Proteger la confidencialidad de los datos y de las acciones requeridas por las autoridades judiciales. La obligación de secreto funcional se extiende a empleados o funcionarios del proveedor u operador, así como a las empresas o personas que le brinden servicios, en concordancia con la obligación de confidencialidad señalada en el Código Procesal Penal.

Los datos de abonado, de localización o de tráfico, en el marco de una investigación penal judicial, podrán ser entregados ante solicitud del Ministerio Público o de la Policía Judicial, si el proveedor de servicios cuenta con el consentimiento de sus clientes, indicado en los términos del contrato de servicio o política de privacidad. En caso contrario, requerirá de autorización judicial. El proveedor podrá requerir que la entrega de la información sea autorizada por un juez penal, para cumplir con su legislación local.

Todo proveedor u operador costarricense de relevancia en servicios electrónicos o de telecomunicaciones deberá hacer un reporte anual de transparencia con respecto a la entrega de información de sus clientes a las autoridades judiciales y clasificada por el tipo de investigación de delitos para el cual fue solicitada.

ARTÍCULO 7. Remoción de contenido en casos de Acoso Cibernético o Pornografía infantil.

Dentro de un máximo de 24 horas posteriores a la interposición de la denuncia por los delitos de acoso cibernético o pornografía infantil, a solicitud del Ministerio Público, un juez deberá resolver la solicitud de remoción del contenido publicado o difundido en la ejecución del delito informático, dirigida al proveedor de servicios electrónicos o al ofensor en cualquier medio que tenga bajo su control.

El juez deberá valorar que, a través de esta medida, no se pueda generar una afectación irreparable a la libertad de expresión y/o al derecho de acceso a la información.

El juez podrá conceder la remoción parcial del contenido, como puede ser la eliminación de datos específicos de un documento o contenido, si considera que con esto se logra un balance entre la protección de los derechos de la víctima y la libertad de expresión.

ARTÍCULO 8. Asistencia mutua en relación con la investigación de delitos informáticos.

El Poder Judicial reglamentará los procesos de asistencia mutua para cumplir con lo requerido con el Convenio de Europa sobre Ciberdelincuencia (Budapest 2001), aprobado mediante ley No.9452 de 26 de mayo de 2017, respetando la legislación vigente.

ARTÍCULO 9. Acceso transfronterizo a datos alojados en el extranjero.

Las autoridades judiciales, dentro del marco de una investigación judicial, podrán:

1. Tener acceso o recibir datos informáticos almacenados en otro país, si se obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos.

2. Tener acceso a datos informáticos almacenados que se encuentren disponibles desde nuestro territorio, con independencia de la ubicación geográfica de dichos datos.

ARTÍCULO 10. Reformas al Código Penal. Refórmanse los artículos 7, 167, 167 bis, 173, 173 bis, 174, 194, 194 bis, 196, 196 bis, 198, 209, 217 bis, 223, 229 bis, 229 ter, 230, 231, 232, 233, 234 236, 263 y 281 del Código Penal No.4573 de 4 de mayo de 1970, cuyos textos dirán:

"Artículo 7.- Delitos internacionales. Independientemente de las disposiciones vigentes en el lugar de la comisión del hecho punible y la nacionalidad del autor, se penará, conforme **con** la ley costarricense, a quienes cometan actos de piratería, terrorismo o su financiamiento, o actos de genocidio; falsifiquen monedas, títulos de crédito, billetes de banco y otros efectos al portador; trafiquen, ilícitamente, armas, municiones, explosivos o materiales relacionados; tomen parte en la trata de **personas**, mujeres o niños; cometan delitos sexuales contra personas menores de edad; se ocupen del tráfico de estupefacientes o de publicaciones obscenas; **cometan delitos informáticos o mediante el uso de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos, o mediante el uso de nuevas tecnologías**. En igual forma se penará a quienes cometan otros hechos punibles contra los derechos humanos y el Derecho internacional humanitario, previstos en los tratados suscritos por Costa Rica o en este Código."

“Artículo 167.- Corrupción de menores o incapaces.

Será sancionado con pena de prisión de tres a ocho años, siempre que no constituya un delito penalizado en formas más grave:

1. A quien permita, promueva o mantenga en una situación o estado de corrupción a una persona menor de edad o incapaz.
2. A quien ejecute, o haga ejecutar a otro, actos eróticos o sexuales prematuros, perversos, antinaturales o excesivos sobre una persona menor de edad o incapaz, o haga participar a una persona menor de edad o incapaz en actos de tal naturaleza, aunque la víctima consienta en participar en ellos.
3. A quien permita o promueva la observación, por parte de personas menores de edad o incapaces, de actos eróticos o sexuales de cualquier índole, incluyendo exhibiciones o espectáculos pornográficos, obscenos, antinaturales o cualquier otro acto de naturaleza similar, ya sea en sitios o locales públicos o privados, aunque las víctimas consientan en observarlos.
4. A quien permita o promueva la presencia de personas menores de edad o incapaces, en sitios o locales, públicos o privados, donde se exhiban espectáculos eróticos, pornográficos, obscenos o antinaturales, aunque las víctimas consientan en estar presentes.”

“**Artículo 167 bis. - Acoso de menores o incapaces.**

Será reprimido con prisión de uno a tres años a quien por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona incapaz o menor de quince años con quien tenga una diferencia de edad de al menos tres años.

La misma pena se impondrá a la persona mayor de edad que suplantando la identidad de un tercero o mediante el uso de una identidad falsa para ocultar su identidad ante la víctima, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos

o audios, con una persona menor de edad o incapaz.

La pena será de dos a cuatro años cuando, en las conductas descritas en los dos párrafos anteriores, el actor procure un encuentro personal en algún lugar físico con una persona menor de edad o incapaz.”

“Artículo 173.-Fabricación, producción o reproducción de pornografía infantil. Será sancionado con pena de prisión de cuatro a ocho años, quien fabrique, produzca o reproduzca, por cualquier medio, material pornográfico infantil. La pena será de cuatro a diez años de prisión si en el material pornográfico aparecen personas menores de siete años.

Será sancionado con pena de prisión de tres a seis años, quien transporte o ingrese en el país este tipo de material.”

“**Artículo 173 bis.-Tenencia de material pornográfico infantil.** Será sancionado con pena de prisión de uno a cuatro años, quien posea material pornográfico infantil. La pena será de tres a seis años de prisión si en el material pornográfico aparecen personas menores de siete años.”

“**Artículo 174.- Difusión de pornografía a menores.** Quien entregue, comercie, difunda, distribuya o exhiba material pornográfico a personas menores de edad o incapaces, será sancionado con pena de prisión de tres a siete años.

Se impondrá pena de tres a ocho años, a quien exhiba, difunda, adquiera, distribuya, financie, ofrezca o comercialice, por cualquier medio y cualquier título, material pornográfico en el que aparezcan personas menores de edad o lo posea para estos fines. La pena será de cinco a diez años de prisión si en el material pornográfico aparecen personas menores de siete años. “

“Artículo 196.- Violación de comunicaciones.

Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino comunicaciones dirigidas a otra persona o sus documentos privados.

Será reprimido con pena de prisión de uno a cuatro años a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.

Será reprimido con pena de prisión de uno a tres años a quien, en perjuicio de una persona física o jurídica, intervenga o capture comunicaciones confidenciales entre dos sistemas informáticos.

Será reprimido con pena de prisión de seis meses a tres años a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.

La pena será de dos a cuatro años de prisión en los siguientes casos:

a) Las conductas sean realizadas por las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

b) Las conductas sean realizadas personas encargadas de administrar o dar soporte al sistema informático, o bien, que en razón de sus funciones tengan acceso a dicho sistema o a los soportes de almacenamiento.

c) La difusión de los documentos o comunicaciones privadas tengan un alcance a una cantidad de personas en medios electrónicos igual o superior al equivalente al 1% de la población nacional.

“Artículo 196 bis.- Violación de datos personales

Será sancionado con pena de prisión de uno a tres años a quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica, almacenados en sistemas informáticos o en soportes de almacenamiento.

La misma pena indicada en el párrafo anterior se impondrá a quien, con peligro a la intimidad o privacidad de una o más personas, se apodere o difunda datos personales sensibles y confidenciales sin el consentimiento del titular de los datos.

Será sancionado con pena de prisión de tres a cinco años a quien copie o se apodere de una base de datos electrónica de datos personales, sin la autorización de los titulares de los datos personales contenidos en ésta o del responsable de la base de datos.

Será sancionado con pena de prisión de seis meses a un año a quien, con peligro o daño para la intimidad o privacidad, por cualquier medio capte u obtenga la ubicación geográfica de una persona, en tiempo real o de forma periódica y sin la autorización del titular del dato, excepto cuando exista orden o sentencia judicial que así lo ordene.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en los tres párrafos iniciales:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema informático, o bien, que en razón de sus funciones tengan acceso a dicho sistema o a los soportes de almacenamiento.

b) Los datos personales vulnerados sean de carácter sensible.
c) Cuando el actor se valga del anonimato para realizar la acción delictiva.”

“Artículo 198.- Captación ilegal de manifestaciones verbales y actos íntimos. Será reprimido, con prisión de seis meses a tres años, a quien, con daño a la intimidad o privacidad y sin consentimiento de los participantes de una comunicación oral, grabe sus manifestaciones verbales, no destinadas al público o que, mediante procedimientos técnicos, escuche manifestaciones privadas que no le estén dirigidas, excepto si existe orden judicial que lo autorice. La misma pena se impondrá a quien instale aparatos, instrumentos o sus partes, con el fin de interceptar o impedir las comunicaciones orales o escritas, logren o no con su propósito.

La misma pena indicada en el párrafo anterior se impondrá a quien capture un acto sexual, con daño a la intimidad o privacidad y sin el consentimiento de todos los participantes del acto.

Será reprimido con prisión de seis meses a dos años a quien, con daño a la intimidad o privacidad, capture las partes íntimas de una persona que no desee mostrarlas en público, ya sea porque las tiene parcialmente cubiertas o porque se encuentra en un lugar privado donde no se sepa observado.”

“Artículo 217 bis.- Estafa informática.
Se impondrá prisión de dos a seis años a 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.

La pena será de tres a diez años de prisión cuando:

1. Las conductas sean cometidas contra sistemas informáticos públicos, bancarios o de entidades financieras.

2. El autor es un empleado encargado de administrar o dar soporte al sistema informático, o bien, que en razón de sus funciones tenga acceso al mismo, o a los soportes de almacenamiento.

3. El monto de lo defraudado excediere de diez veces el salario base."

"Artículo 223.- Apropiación y retención indebidas.
Se impondrá la pena establecida en el artículo 216 del Código Penal, según el monto de lo apropiado o retenido al que, teniendo bajo su poder o custodia una cosa mueble, un valor ajeno o **activo digital**, por un título que produzca la obligación de entregar o devolver, se apropiare de ello o no lo entregare o restituyere a su debido tiempo, en perjuicio de otro. Si no hubiere apropiación sino uso indebido de la cosa, con perjuicio ajeno, la pena se reducirá, a juicio del juez.

En todo caso, previamente el imputado será prevenido por la autoridad que conozca del asunto, para que, dentro del término de cinco días hábiles, devuelva o entregue el bien y, si lo hiciere no habrá delito, sin perjuicio de las acciones civiles que a las que pudiere recurrir el dueño."

“Artículo 229 bis.- Daño informático

Siempre que no constituya delito con una pena superior, se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de **otra persona**, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en soportes de almacenamiento.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.”

“Artículo 229 ter.- Sabotaje informático

Se impondrá pena de prisión de uno a seis años al que destruya, altere, entorpezca o inutilice la información contenida en una base de datos electrónica, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema automatizado de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de tres a ocho años de prisión 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 informático, o bien, que en razón de sus funciones tenga acceso a dicho sistema, o a los soportes de almacenamiento.

c) El sabotaje afecte infraestructura crítica de Costa Rica o un país extranjero.

d) El sabotaje atente contra un servicio digital que utilice una cantidad de personas igual o superior al equivalente del 1% de la población nacional.”

“Artículo 230.- Suplantación de identidad.

Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica, marca o aplicación informática, en cualquiera red social, sitio de internet, medio electrónico, tecnológico de información o tienda digital de aplicaciones informáticas.”

“Artículo 231.- Espionaje industrial o comercial.

Se impondrá prisión de dos a seis años 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 232.- Instalación o propagación de programas informáticos maliciosos.

Será sancionado con prisión de uno a siete años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema informático.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale o ejecute un programa informático malicioso en un sistema informático.

b) A quien, sin autorización, instale programas dañinos en sitios de Internet legítimos, con el fin de convertirlos en 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 atacantes.

d) A quien distribuya herramientas informáticas diseñadas 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.

La pena será de tres a nueve años de prisión 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 o infraestructura crítica nacional o extranjera.

iii) Obtenga el control a distancia de un sistema informático para que forme 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**.**

vii) Tenga la capacidad de copiar una base de datos electrónica de datos personales.”

“Artículo 233.- Suplantación de páginas electrónicas.
Se impondrá pena de prisión de uno a tres años a quien, en perjuicio **de otra persona**, suplante sitios legítimos de la red de Internet.

La pena será de dos a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet, capture información confidencial de una persona física o jurídica para beneficio propio o de otra persona.”

“Artículo 234.- Facilitación del delito informático.
Siempre que no constituya delito con una pena superior, se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito informático o del cibercrimen.”

“Artículo 236.- Difusión de información falsa.
Será sancionado con pena de uno a cuatro años de prisión a quien fabrique **y** difunda, a través de medios informáticos, una noticia falsa capaz de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

La misma pena indicada en el párrafo anterior se impondrá a quien fabrique **y** difunda, a través de medios informáticos, una noticia falsa con el fin de afectar la decisión del electorado en un proceso de plebiscito, referéndum o electoral nacional o extranjero.

La pena será de tres a seis años de prisión cuando a raíz de la difusión de la noticia falsa sobreviniere peligro de muerte para una o varias personas.”

“Artículo 263.- Entorpecimiento de servicios públicos.
Será reprimido con prisión de seis meses a dos años, **a la persona que**, sin crear situación de peligro común, impidiere, estorbare o entorpeciere el normal funcionamiento de los transportes por tierra, agua y aire a los servicios públicos de comunicación o de sustancias energéticas.

La pena será de tres a ocho años si las acciones descritas en el párrafo anterior fuesen cometidas mediante el uso de dispositivos o artificios tecnológicos, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema informático, o que en razón de sus funciones tengan acceso a dichos sistemas o soportes de almacenamiento.”

“Artículo 281.- Asociación ilícita.
Será reprimido con prisión de uno a seis años, quien tome parte en una asociación de dos o más personas para cometer delitos, por el solo hecho de ser miembro de la asociación.

La pena será de cuatro a ocho años de prisión si el fin de la asociación es cometer actos de terrorismo, secuestro extorsivo, cibercrímenes o delitos en que se vean involucrados menores o incapaces.”

ARTÍCULO 11. Adición al artículo 209 del Código Penal. Adiciónase un inciso 8 al artículo 109 del Código Penal No.4573 de 4 de mayo de 1970, el cual dirá:

“Artículo 209. Hurto Agravado

Se aplicará prisión de uno a nueve años, si el valor de lo sustraído no excede de cinco veces el salario base, y de cinco a diez años, si fuere mayor de esa suma, en los siguientes casos:

[...]

8) Si se hiciere a través de la vulneración de sistemas de autenticación o mediante el uso de claves de acceso, tarjetas magnéticas, electrónicas, llaves inalámbricas o dispositivos similares, chips, brindados por las nuevas tecnologías, incluyendo tarjetas bancarias de crédito, débito, firmas electrónicas, certificados digitales o de cualquier otra índole, que hubieren sido sustraídos, hallados, vulnerados, clonados, retenidos, copiados o reproducidos por cualquier medio."

ARTÍCULO 12. Adiciónanse al Código Penal No.4573 de 4 de mayo de 1970 los artículos 194, 194 bis, 196 ter, 196 quater, 217 ter, 232 bis, 233 bis que dirán:

"Artículo 194 - Acoso cibernético

Será reprimido con pena de prisión de seis meses a tres años a quien acose a una o varias personas y, de este modo, altere gravemente el desarrollo de su vida cotidiana, a través alguna de las siguientes acciones:

1. El envío de mensajes o publicaciones por medios electrónicos, reiterado o insistente, de contenido ofensivo, o con información de la víctima o de sus seres queridos, que le hagan sentir vigilada.

2. La adquisición, de forma insistente o reiterada, de bienes o servicios a nombre de la víctima sin su consentimiento.

3. La invitación pública a terceras personas a que se comuniquen o agredan a la víctima, sin conocimiento o la autorización de ésta.

4. La difusión de imágenes, audio o vídeos de carácter sexual o pornográfico, donde aparezca o tenga participación la víctima.

5. La difusión de imágenes, audios o vídeos de carácter sexual o pornográfico donde falsamente se le atribuya a la víctima participar o aparecer en estos.

6. El control remoto o a distancia, reiterado o insistente, de los dispositivos de la víctima que cuenten con acceso a Internet u otras redes, y sin autorización de la persona afectada.

7. La publicación o envío de mensajes con amenazas hacia la víctima o sus familiares, en una red social, aplicación de mensajería, blog o medio social dirigido al público general.

8. De forma insistente o reiterada vigile, persiga o busque cercanía física con la víctima.

La pena será de dos a cuatro años, cuando:

1. A raíz de las conductas desplegadas por el actor la víctima atente contra su vida o integridad física, o bien, que afecte su salud psicológica.

2. Las conductas realizadas por el actor tengan un alcance a una cantidad de personas en medios electrónicos igual o superior al equivalente al 1% de la población nacional.

3. Las conductas realizadas por el actor se hagan a través de la creación de uno o más perfiles falsos en medios sociales.

4. Las víctima sea una persona menor de edad o incapaz.”

“Artículo 194 bis - Ciberacoso sexual.

Siempre que no constituya el delito de acoso cibernético, será reprimido con pena de treinta a cincuenta días multa a la persona que, de forma no solicitada, reiterada y fuera del marco de una comunicación recíproca de índole sexual o erótica, envíe mensajes con propuestas sexuales o contenido pornográfico, a otra persona, con la quien no tenga una relación de pareja o índole sexual."

"Artículo 196 ter.- Difusión o tráfico de contraseñas o vulnerabilidades.
Será reprimido con pena de prisión de seis meses a dos años de prisión a quien, en perjuicio de otra persona, difunda o comercie una o varias contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. La pena será de tres a cinco años de prisión cuando la información filtrada provenga de bases de datos que afecte a un número de personas igual o superior al equivalente al 1% de la población nacional.

Será reprimido con pena de prisión de un año a cuatro años de prisión a quien adquiera, compre, consiga o venda vulnerabilidades de una aplicación o sistema informático que permitan la comisión de un delito informático."

"Artículo 196 quater.- Acceso llícito.
Siempre que no constituya delito con una pena superior, será reprimido con pena de seis meses a un año de prisión a quien, evadiendo medidas de seguridad y con fines maliciosos, acceda a un sistema informático, sin la autorización del titular."

"Artículo 217 ter.- Compras ilícitas mediantes tarjetas.
Será sancionado con pena de prisión de dos a cinco años de prisión a quien adquiera bienes o servicios, a través del uso de una tarjeta de crédito o de débito no expedida en su favor, o mediante el uso de otro medio de pago electrónico, sin la autorización del titular."
"Artículo 232 bis- Abuso de dispositivos.

Se impondrá pena de prisión de uno a cinco años a quien distribuya, produzca, venda, compre, obtenga para su utilización o importe un dispositivo o programa informático diseñado o adaptado principalmente para la comisión de delitos informáticos."

"Artículo 233 bis.- Ingeniería social.
Siempre que no constituya delito con una pena superior, se impondrá pena de prisión de seis meses a dos años a quien, mediante engaño, capture u obtenga datos personales o información confidencial apta para la comisión de un delito informático."

ARTÍCULO 13. Adiciónese el inciso k) al artículo 244 del Código Procesal Penal, el texto dirá:

"Artículo 244.- Otras medidas cautelares. Siempre que las presunciones que motivan la prisión preventiva puedan ser evitadas razonablemente con la aplicación de otra medida menos gravosa para el imputado, el tribunal competente, de oficio o a solicitud del interesado, deberá imponerle en su lugar, en resolución motivada, alguna de las alternativas siguientes:
[...]
k) La prohibición de usar un ordenador, sistema o aplicación informática si existe peligro de la comisión de uno o más delitos informáticos. Si la prohibición de la utilización de un ordenador o sistema informático puede dejar sin medios para subsistir al imputado o afecte de forma grave el derecho de acceso a la información, se podrá instalar una aplicación informática controlada por las autoridades que genere un registro de las acciones realizadas por el imputado en el ordenador, siempre que el mecanismo no capture comunicaciones privadas."

ARTÍCULO 14. Se reforma el artículo 9 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y sus reformas, No.7425 de 09 de agosto de 1994, cuyo texto se leerá como sigue:

“Artículo 9.- Autorización de intervenciones.
Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: **delitos informáticos, delitos computacionales con penas de hasta 4 años de prisión;** secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, No.7786 de 30 de abril de 1998 y sus reformas.

En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente Ley; cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva.”

ARTÍCULO 15. Adiciónanse los incisos 3) y 4) al artículo 23 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones No.7425 de 09 de agosto de 1994, cuyo texto dirá:

“Artículo 23.- Obligaciones de los responsables de las empresas de comunicación.

Serán obligaciones de los funcionarios responsables de las empresas o instituciones públicas y privadas a cargo de las comunicaciones:

[...]

3.- Conservar los datos de tráfico y datos de localización de las telecomunicaciones, por un periodo mínimo de cuatro años o hasta su prescripción legal.

4.- Mantener un sistema de bitácoras actualizadas que permitan identificar una dirección ip con el abonado del servicio, en un intervalo de tiempo específico.”

Rige a partir de su publicación.

