



Asamblea Nacional
Secretaría General
TRÁMITE LEGISLATIVO
2017-2018

PROYECTO DE LEY: **558**

LEY:

GACETA OFICIAL:

TÍTULO: QUE MODIFICA Y ADICIONA ARTÍCULOS AL CÓDIGO PENAL, RELACIONADOS CON EL CIBERCRIMEN.

FECHA DE PRESENTACIÓN: **27 DE SEPTIEMBRE DE 2017.**

PROPONENTE: **LICDA. KENIA I. PORCELL D., PROCURADORA GENERAL DE LA NACIÓN.**

COMISIÓN: **GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES.**



República de Panamá
Procuraduría General de la Nación

Panamá, 18 de septiembre de 2017
PGN-FSL-226-17

Honorable Diputada
Yanibel Ábrego Smith
Presidenta de la Asamblea Nacional
E. S. D.

Señora Presidenta:

En uso de la iniciativa legislativa que me confiere el artículo 165 de la Constitución Política de la República de Panamá, presento por su conducto al Pleno de este Órgano del Estado, el Proyecto de Ley **“Que modifica y adiciona artículos al Código Penal, relacionados con el Cibercrimen”**, el cual amerita las siguientes consideraciones.

EXPOSICIÓN DE MOTIVOS

Hoy en día la tecnología de la información (TIC's) y la comunicación ha evolucionado, conllevando múltiples beneficios, sin embargo, también nos somete a todo tipo de riesgos. Para evitar estos debemos actualizarnos y prepararnos en lo concerniente a la seguridad informática para enfrentar las tecnologías utilizadas indebidamente.

El impacto de estas tecnologías, ha implicado una transformación en la forma de convivir en sociedad, en la que se destaca la concepción de un mundo globalizado, de un “ciberespacio” y de verdaderas “culturas cibernéticas”.

Ahora bien, la evolución o cambios informáticos transforman e impactan el Derecho Penal tradicional y, como consecuencia de ello, se deben adecuar los tipos penales que hoy día quedan en la impunidad, por ser conductas no reguladas en la Ley.

En este sentido, los delitos informáticos o cometidos a través de medios informáticos son modalidades delictivas, que incluyen una amplia variedad de categorías de crímenes tradicionales y no tradicionales, que se realizan por medio o a través de estructuras electrónicas ligadas a un sinnúmero de herramientas informáticas, que buscan no sólo infringir sistemas informáticos sino dañar todo lo que se encuentren en el ámbito tecnológico.

SECRETARÍA GENERAL

Fecha: 27/9/17

Hora: 6:00 pm

De: _____

Para: _____

Asunto: _____

Revisado por: _____

Revisado por: _____

Estas nuevas propuestas y modificaciones se requieren con carácter de urgencia, en virtud que en la actualidad carecemos de estos tipos penales que exige la gran demanda de nuevas conductas, que no están debidamente reglamentadas, y podamos cumplir a cabalidad con las investigaciones con un perfil de delitos de alta tecnología y responder a la sociedad con la imposición de una pena acorde al responsable de esa conducta.

La República de Panamá, no escapa a esta realidad. Uno de los propósitos de este Proyecto de Ley, es regular a la luz de la ley sustantiva, la protección de la información y tipificar conductas delictivas, relacionadas a las nuevas tendencias que incluyen desde el acceso ilegal a sistemas informáticos, suplantación de identidad, interceptación ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datos informáticos), extorsión, fraudes electrónicos, estafas, ataques a sistemas informáticos, ataques realizados por *hackers*, captura de datos bancarios (*phishing*, *pharming*), computadoras zombies (*botnets*), violación de los derechos de autor, pornografía infantil, pedofilia, denegación de servicios, ciberacoso (*ciberbullying* y *cibergrooming*), violación de información confidencial, acoso y muchos otros. Todo realizado a través de redes informáticas, utilizando para ello la instalación de códigos, de gusanos, de archivos maliciosos, de *spam* (correo basura), de ataque masivos a servidores de Internet y mediante generación de virus.

Conceptos modernos, como el de Infraestructura Crítica del Estado, protección de datos personales, deben desarrollarse su extensión, para ser interpretado como bien jurídico tutelado dentro del análisis dogmático de toda figura delictiva, para lograr así una protección integral.

En ese sentido, a nivel internacional existen tanto herramientas jurídicas para la persecución de los delitos informáticos como organismos especializados para su investigación. Así podemos mencionar el Convenio de Budapest de 2001 sobre la Ciberdelincuencia, el cual la República de Panamá aprobó a inicios del mes de septiembre de 2013. El mismo es un instrumento legal que tiene como propósito desarrollar las herramientas de investigación y cooperación en materia de cibercrimen. Una vez que se ha suscrito este convenio, nace la necesidad de adoptar las medidas legislativas requeridas con el fin de tipificar toda conducta que afecte los medios informáticos.

Además, para cumplir con los estándares internacionales de Seguridad Informática, la República de Panamá creó a través del Decreto Ejecutivo N° 709 del 26 de septiembre de 2011, el Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información, adscrito a la Autoridad para la Innovación Gubernamental o AIG, denominado CSIRT PANAMA, para atender todos los incidentes que involucren ataques contra la Seguridad Informática del Estado,

quienes también fungen como auxiliares del Ministerio Público en la investigación de este tipo de incidentes.

La propuesta efectuada a través del presente Proyecto de Ley adecúa nuestro derecho positivo a nuevas conductas punibles de carácter tecnológico.

PROYECTO DE LEY N° 558

COMISIÓN DE GOBIERNO, JUSTICIA Y ASUNTOS CONSTITUCIONALES
PROYECTO DE LEY

De de de 2017

ASAMBLEA NACIONAL SECRETARIA GENERAL	
Presentación	27/9/17
Hora	6:00 pm
A Debate	

Que modifica y adiciona artículos al Código Penal, relacionados con el Cibercrimen

**LA ASAMBLEA NACIONAL,
EN USO DE SUS FACULTADES CONSTITUCIONALES Y LEGALES,**

DECRETA:

Artículo 1. Se adiciona el numeral 15 al **artículo 88 del Código Penal**, así:

Artículo 88. Son circunstancias agravantes comunes las siguientes:

...

15. Cuando para la realización del hecho punible se utilice un sistema informático, sistema electrónico, datos informáticos o comunicación electrónica.

...

Artículo 2. El **artículo 166 del Código Penal**, queda así:

Artículo 166. Quien posea o **acceda** legítimamente a una correspondencia, **datos informáticos**, grabación o documentos privados y de carácter personal, no destinados a la publicidad, aunque le hubieran sido dirigidos, y los haga públicos sin la debida autorización y de ello pudiera resultar un perjuicio, será sancionado con doscientos a quinientos días-multa o arresto de fines de semana.

No se considerará delito la divulgación de **datos informáticos** o documentos indispensables para la comprensión de la historia, las ciencias, las artes o **cualquier información que sea de interés público y que se divulgue, en ejercicio legítimo de la libertad de prensa.**

Si media el perdón expreso de la víctima, se ordenará el archivo de la causa.

Artículo 3. El **artículo 184 del Código Penal**, queda así:

Artículo 184. Quien fabrique, elabore por cualquier medio o produzca material pornográfico o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya **a través de un sistema informático o sistema electrónico** o cualquier medio masivo de comunicación o información nacional o internacional, presentando o

representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de cinco a diez años.

La pena será de diez a quince años de prisión si la víctima es una persona menor de catorce años, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro.

Artículo 4: Se adiciona el artículo 184-A al Código Penal, así:

Artículo 184-A. Quien, con la finalidad de cometer delitos Contra la Libertad e Integridad Sexual, utilice cualquier medio, inclusive un sistema informático, sistema electrónico o comunicación electrónica para contactarse o comunicarse con una persona menor de edad, persona con discapacidad que no le permita resistirse, será sancionado con pena de prisión de cuatro a seis años.

La pena será de seis a ocho años de prisión si la víctima es una persona menor de catorce años.

Artículo 5. El artículo 185 del Código Penal, queda así:

Artículo 185. Quien posea, obtenga o acceda a través de un sistema informático o sistema electrónico, para uso propio, material pornográfico que contenga la imagen, real o simulada, de personas menores de edad, será sancionado con pena de prisión de tres a cinco años.

Artículo 6. Se adiciona el artículo 195-A al Código Penal, así:

Artículo 195-A. Quien utilice indebidamente, un medio de comunicación electrónica o sistema informático que pertenezca a otra persona natural o jurídica, con la finalidad de cometer o colaborar con un delito, será sancionado con pena de cuatro a seis años de prisión.

Artículo 7. Se adiciona el artículo 200-A al Código Penal, así:

Artículo 200-A. La sanción prevista en el artículo anterior se aplicará a quien utilizando sistemas informáticos o sistemas electrónicos o comunicaciones electrónicas, difunda, divulgue, reproduzca, retransmita o traspase datos informáticos que afecten o atenten la integridad física, mental o emocional de otro miembro de la familia.

Artículo 8. Se adiciona el artículo 204-A al Código Penal, así:

Artículo 204-A. Quien a través de un sistema informático, sistema electrónico, comunicación electrónica, difunda, divulgue, reproduzca, retransmita o traspase datos informáticos que afecten o atenten la integridad física, mental o emocional de una persona menor de edad, será sancionado con pena de dos a cuatro años de prisión.

Si el autor es ascendiente, pariente cercano, encargado de la guarda, crianza, y educación o tutor o encargado de su cuidado o atención, o quien interviene en el proceso de educación, formación y desarrollo integral, la sanción será aumentada de una tercera parte a la mitad.

Igual pena se le aplicará si la víctima es una persona con discapacidad.

Artículo 9. El artículo 224 del Código Penal, queda así:

Artículo 224. Quien, sin consentimiento del propietario, proveedor, concesionario o administrador, utilice, consuma, **bloquee, desbloquee** o capte energía, agua, telecomunicación, señal de telecomunicación y video, equipo terminal de cable, satélite, parabólica o altere cualquier elemento de medición o de control de estos, será sancionado con prisión de uno a dos años.

La pena será de dos a cuatro años de prisión para quien transmita, retransmita o distribuya.

Artículo 10. El artículo 226 del Código Penal, queda así:

Artículo 226. Quien, para procurarse para sí o para un tercero un provecho ilícito, **ingrese, altere, borre, modifique** o manipule datos, o interfiera con el funcionamiento de un sistema informático o **sistema electrónico**, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión.

La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base datos, redes o sistema informático o **sistema electrónico** o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada.

Artículo 11. Se adiciona el artículo 226-A al Código Penal, así:

Artículo 226-A. Quien, con la finalidad de cometer algún delito, cree una identidad falsa o suplante la identidad de una persona natural o jurídica, utilizando la firma electrónica o los datos contenidos en un sistema informático, sistema electrónico o comunicación electrónica, será sancionado con pena de dos a cuatro años de prisión.

Artículo 12. El artículo 243 del Código Penal, queda así:

Artículo 243. Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita, o haga uso indebido de dineros, valores u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que se le hayan confiado, o realice esas conductas a través de **un sistema informático o sistema electrónico** o de forma fraudulenta, será sancionado con prisión de cuatro a seis años.

La sanción será de seis a ocho años de prisión, cuando el hecho punible es cometido por un **servidor público**, empleado, trabajador, directivo, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno.

Artículo 13. El artículo 289 del Código Penal, queda así:

Artículo 289. Quien indebidamente, **sin la debida autorización o excediendo la que posea, infringiendo los controles de seguridad**, ingrese, utilice o permanezca

conectado, a un sistema informático o **electrónico**, será sancionado con prisión de dos a cuatro años.

Igual sanción se le impondrá a quien indebidamente revele o difunda los datos informáticos confidenciales obtenidos.

La pena será de seis a ocho años cuando se trate de infraestructura crítica del Estado.

Artículo 14. Se adiciona el **artículo 289-A al Código Penal, así:**

Artículo 289-A. Quien dañe u obstaculice, total o parcialmente, el funcionamiento de un sistema informático o electrónico mediante la alteración, deterioro, introducción, transmisión, borrado o supresión de datos informáticos, será sancionado con prisión de cuatro a seis años.

Cuando alguna de las conductas anteriores sea realizada contra infraestructura crítica del Estado, la pena será de cuatro a diez años.

Artículo 15. Se adiciona el **artículo 289-B al Código Penal, así:**

Artículo 289-B. Quien sin autorización del destinatario inicie la transmisión de múltiples mensajes electrónicos desde o a través de un sistema informático o electrónico, con el propósito de engañar, confundir, causar daño o la destrucción de un sistema informático o electrónico, será sancionado con prisión de cuatro a seis años.

Igual sanción se aplicará a quien:

1. Utilice un sistema informático o electrónico protegido para enviar o retransmitir múltiples mensajes electrónicos o para ocultar el origen de tales mensajes.
2. Falsifique información contenida en encabezados de mensajes electrónicos e intencionalmente inicie su transmisión.

Artículo 16. El **artículo 290** del Código Penal, queda así:

Artículo 290. Quien **dañe**, borre, altere, obstruya, interrumpa, interfiera o niegue el acceso a datos informáticos contenidos en un sistema informático, sistema electrónico o cualquier medio de almacenamiento, será sancionado con pena de dos a cuatro años de prisión.

Artículo 17. Se adiciona el **artículo 290-A al Código Penal, así:**

Artículo 290-A. Quien sin autorización se apodere o utilice datos almacenados en un sistema informático o sistema electrónico, total o parcialmente, será sancionado con prisión de cuatro a seis años.

La pena será de seis a ocho años cuando se trate de infraestructura crítica del Estado.

Artículo 18. Se adiciona el **artículo 290-B al Código Penal, así:**

Artículo 290-B. Quien sin autorización intercepte u obstaculice la transmisión de datos informáticos en tránsito pertenecientes a otro, para beneficio propio o de un tercero, será

sancionado con pena de cuatro a seis años de prisión.

Artículo 19. Se adiciona el **artículo 290-C al Código Penal, así:**

Artículo 290-C. Quien sin autorización inhabilite, desactive o invalide los controles de accesos de forma parcial o total de un sistema informático, sistema electrónico, o sus componentes, será sancionado con cuatro a seis años de prisión.

Artículo 20. El **artículo 291** del Código Penal, queda así:

Artículo 291. Las conductas descritas en los artículos precedentes se agravarán de un tercio a una sexta parte de la pena si se cometen contra un sistema informático, **sistema electrónico, datos informáticos** de:

1. Oficinas públicas o bajo su tutela.
2. Instituciones públicas, privadas o mixtas que prestan un servicio público.
3. Bancos, aseguradoras y demás instituciones financieras y bursátiles.

También se agravará la pena en la forma prevista en este artículo cuando los hechos sean cometidos con fines lucrativos.

Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente Capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código.

Artículo 21. El **artículo 292** del Código Penal, queda así:

Artículo 292. Cuando las conductas descritas en el presente Capítulo las comete la persona encargada o responsable de los **datos informáticos, sistema informático o sistema electrónico**, o la persona autorizada para acceder a estos, o las cometió utilizando información privilegiada, la sanción se agravará entre una sexta y una tercera parte.

Artículo 22. Se adiciona el **artículo 292-A al Código Penal, así:**

Artículo 292-A. Quien posea, utilice, distribuya, fabrique, diseñe, modifique, programe, venda, importe, exporte, custodie, almacene, trafique, adquiera, envíe o elabore sin autorización o de forma ilícita, claves, contraseñas, códigos de acceso, programas informáticos, equipos, materiales o dispositivos cuyo uso esté destinado a la alteración o destrucción de datos informáticos o a la comisión de delitos, será sancionado con cuatro a seis años de prisión.

Artículo 23. Se adiciona el **artículo 292-B al Código Penal, así:**

Artículo 292-B. Cuando de las conductas descritas en los artículos anteriores, se revelen datos o contenidos confidenciales de todo tipo, se afecte la intimidad o la privacidad de las personas, será sancionado con seis a ocho años de prisión.

Artículo 24. Se adiciona el **artículo 292-C al Código Penal, así:**

Artículo 292-C. Cuando algunas de las conductas descritas en este título sea cometida por un servidor público la sanción se aumentará de una tercera parte a la mitad.

Artículo 25. Se adiciona el artículo 365-A al Código Penal, así:

Artículo 365-A. Quien, para cometer alguno de los delitos contemplados en el presente título, utilice un sistema informático, sistema electrónico, comunicación electrónica, que afecte la infraestructura crítica del Estado, se le aumentará la pena de una tercera a una sexta parte.

Artículo 26. Se adiciona el Capítulo VI al Título Primero del Libro Tercero del Código Procesal Penal, que corresponde a los artículos 338-A, 338-B, 338-C, 338-D, 338-E, 338-F, así:

Capítulo VI

Actos de investigación Necesarios para la Obtención de Evidencias Digitales

Artículo 338-A: Los actos de investigación para la obtención de evidencias digitales, deberán considerar los presupuestos contenidos en la Constitución Política de la República de Panamá, los instrumentos jurídicos internacionales que versen sobre garantías fundamentales y derechos humanos, que sean ratificados por la República de Panamá, así como las garantías, principios y reglas que fundamentan el presente Código.

Artículo 338-B: El Ministerio Público podrá ordenar a cualquier persona física o jurídica, la conservación de la integridad de los datos informáticos concretos, almacenados en un sistema informático que esté bajo su disposición cuando tenga motivos suficientes para considerar que puedan ser alterados o suprimidos y afectar así el resultado de una investigación. La medida no podrá exceder de noventa días y será prorrogable por igual período, si se mantienen los motivos que fundamentaron la orden.

La persona requerida, una vez reciba la comunicación respectiva, deberá ejecutar los actos necesarios que garanticen la preservación, inmediata, de los datos en cuestión y estará obligado a mantener secreto bajo el apercibimiento de incurrir en delito Contra la Administración de Justicia.

Cuando se trate del aseguramiento o conservación de datos relativos al tráfico de comunicaciones, si el proveedor de servicios requerido advierta que en la comunicación objeto de la investigación han participado otros proveedores de servicios, informará a la autoridad competente que haga el requerimiento, inmediatamente, para que adopte las medidas necesarias.

Artículo 338-C: El Ministerio Público podrá ordenar a cualquier persona física o jurídica, que presente, remita o entregue datos almacenados en un sistema informático que este bajo su poder o control y que se vinculen con la investigación de un delito concreto. Asimismo, podrá ordenar a toda persona física o jurídica que preste un servicio de comunicaciones o a los proveedores de servicios de internet de cualquier tipo, la entrega de datos de los usuarios o abonados o los datos de identificación y facturación

con los que cuente. La orden podrá contener la indicación de que la medida deberá mantenerse en secreto bajo el apercibimiento de sanción penal. Estas medidas serán ejecutadas por el agente de instrucción, salvo las excepciones contempladas en la legislación vigente, en las cuales se exija la autorización judicial.

Artículo 338-D: Con fundamento en lo dispuesto en los tratados y convenciones internacionales ratificados por Panamá, las respectivas autoridades pueden acceder o recibir datos informáticos almacenados en un sistema informático, ubicado en otro Estado, cuando éstos estén a disposición del público, por medio de un sistema informático ubicado en Panamá, con el consentimiento legal y voluntario de la persona legalmente autorizada a revelarlos, en ese país.

Artículo 338-E: Para la obtención, en tiempo real, de datos de tráfico de comunicaciones electrónicas o la interceptación de datos informáticos de contenido, regirá lo dispuesto en el artículo 311 de este Código.

Artículo 338-F: En caso de cooperación internacional las solicitudes de aseguramiento de datos, solicitudes de presentación de datos, de obtención o confiscación, de acceso libre a datos de fuente abierta y asistencia mutua para obtención de datos sobre el tráfico e interceptación de comunicaciones, se estará a lo dispuesto en tratados y convenciones internacionales ratificados por Panamá. También se tomará en cuenta el derecho a la intimidad y a la confidencialidad de ciertos datos protegidos también por tratados y convenciones en materia de derechos humanos, que haya ratificado Panamá.

Artículo 27. La presente Ley modifica los artículos: 166, 184, 185, 224, 226, 243, 289, 290, 291, 292; adiciona el numeral 15 al artículo 88 y los artículos: 184-A, 195-A, 200-A, 204-A, 226-A, 289-A, 289-B, 290-A, 290-B, 290-C, 292-A, 292-B, 292-C, 365-A, al Texto Único del Código Penal. Además, adiciona el Capítulo VI al Título Primero del Libro Tercero del Código Procesal Penal, que corresponde los artículos 338-A, 338-B, 338-C, 338-D, 338-E, 338-F.

Artículo 28. Esta Ley comenzará a regir el día siguiente al de su promulgación.

Propuesto a la consideración de la Asamblea Nacional, hoy 10 de agosto de 2017, por la suscrita Kenia I. Porcell D., Procuradora General de la Nación de conformidad con el literal c, numeral 1 del artículo 165 de la Constitución Política de la República.



Kenia I. Porcell D.
Procuradora General de la Nación

