Panamá:

UN PAÍS CON LA NECESIDAD DE UNA LEGISLACIÓN SOBRE CIBERCRIMEN

Sara Fratti

Portada: Violeta Cereceda
Diagramación: Constanza Figueroa.
Edición: Marianne Díaz
Coordinación: Diego Morales
Autoría: Sara Fratti
Revisión: Lia Hernández

Junio 2018.

Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- es una organización sin fines de lucro basada en la Ciudad de Panamá, que buscar fortalecer los Derechos Humanos en el ecosistema digital en Centroamérica.

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción la libertad de expresión, el acceso a la cultura y la privacidad.

INTRODUCCIÓN.

El vertiginoso desarrollo de las nuevas Tecnologías de la Información y Comunicación de los últimos años han facilitado muchos aspectos de la vida cotidiana del ser humano. Sin embargo, este despliegue también ha incidido en un repunte en los índices de criminalidad asociados al ciberespacio.

El creciente acceso a Internet y las tecnologías han requerido determinar regulaciones jurídicas, desde el reconocimiento de los Derechos Humanos en línea hasta la tipificación de delitos cibernéticos. Sin embargo, esta tarea no ha sido fácil, derivado de la dificultad de determinar diferentes aspectos de la comisión y persecución de los ciberdelitos.

Como consecuencia, el Consejo de Europa tomó la decisión de iniciar el proceso para determinar un catálogo de ciberdelitos y lograr así una estandarización para la persecución y sanción penal de estas conductas, es así como en 2001 se aprobó el primer tratado internacional que regula las conductas delictivas cometidas en el ciberespacio, el Convenio sobre la Ciberdelincuencia.

El presente informe pretende realizar un análisis del proceso actual de la implementación del Convenio de Budapest en el marco jurídico de Panamá, resaltando las debilidades en los proyectos de reforma de la legislación nacional, en materia sustantiva y procesal.

4 —

ANTECEDENTES EN PANAMÁ.

El Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, aprobado por el Consejo de Europa el 23 de noviembre de 2001, es el primer tratado internacional regula los delitos cometidos en el ciberespacio.

Este Convenio posee como objetivos principales brindar estándares en materia de Derecho Penal, establecer procedimientos adecuados al entorno digital y establecer mecanismos para la cooperación internacional en materia de cibercriminalidad. Lo cual, permitirá establecer criterios para la investigación y persecución de estos delitos en todo el mundo.

Con base en lo anterior, el Convenio de Budapest posee dos partes, por un lado regula aspectos del Derecho Penal Sustantivo estableciendo un catálogo de delitos, y por el otro establece las normas relativas al Derecho Procesal Penal. Lo cual permitirá una estandarización normativa y procedimental en materia de ciberdelincuencia, que facilitará en su momento la persecución penal y sanción de estos delitos.

El Convenio de Budapest fue abierto para firma de los Estados miembros del Consejo de Europa y los Estados no miembros, lo cual ha permitido que algunos Estados de América Latina y el Caribe se adhieran al texto del Convenio, el cual se encuentra vigente desde el 1 de julio de 2004.

Una de las principales críticas al Convenio de Budapest, es que los Estados no miembros del Consejo de Europa, principalmente los Estados en vías de desarrollo, no pudieron participar en las negociaciones, tampoco establecer los criterios sustantivos y procesales en materia de ciberdelincuencia.
Antecedentes en Panamá.

El Código Penal de la República de Panamá, aprobado mediante Ley 14 del 18 de mayo de 2007, en su Título VIII, sobre los delitos contra la “Seguridad Jurídica de los Medios Electrónicos” regula los delitos contra la seguridad informática. Del artículo 289 al 292 regula las siguientes conductas delictivas y sus respectivas penas: a) ingresar o utilizar de bases de datos, red o sistemas informáticos; y, b) apoderar, copiar, utilizar o modificar datos en tránsito o contenidos en bases de datos o sistemas informáticos, o interferir, interceptar, obstaculizar o impedir la transmisión. Además, determina ciertas conductas como circunstancias agravantes que aumentan la pena de prisión.

La carencia en la categorización adecuada de tipos penales que exigen la gran demanda de nuevas conductas que no se encuentran debidamente reglamentadas, como consecuencia no se puede cumplir con el desarrollo de investigaciones dentro procesos penales en los que se analizan delitos que utilizan alta tecnología y lograr la imposición de una sanción acorde al responsable de dicha conducta.

La República de Panamá, no escapa de la realidad mundial con lo que respecta a una digitalización, no solo de la información, sino de las conductas delictivas como tal, se veía acechada por el anonimato de grupos delictivos, sin el mecanismo coercitivo de una pena luego de una investigación. Peor aún, no tenía la capacidad de solicitar ayuda a otros Gobiernos, ya que para poder acceder a una solicitud de esta naturaleza, se requiere que dentro de la legislación nacional se encuentren regulados estos tipos penales.

En Panamá se creó en el año el 2011 un CSIRT[1] (Computer Security Incident Response Team, por sus siglas en inglés) bajo la estructura gubernamental de la Autoridad Nacional para la Innovación Gubernamental, creado a través del Decreto Ejecutivo No.709 del Ministerio de Presidencia[2]. El CSIRT-Panamá se encarga prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país.

Desde el 12 de marzo de 2013, Panamá posee una Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas[3], la cual fue aprobada por el Consejo Nacional para la Innovación Gubernamental. La Estrategia Nacional establece una serie de acciones para mejorar la ciberseguridad, así como proteger las infraestructuras vitales del país. Sin embargo, la misma no está siendo implementada por las entidades encargadas, por falta de voluntad política.

La Asamblea Nacional de Panamá aprobó el Convenio sobre la Ciberdelincuencia a través de la Ley 79 del 22 de octubre de 2013, que fue publicada en la Gaceta Oficial No. 27403-A del 25 de octubre del mismo año. Panamá aprobó el texto del Convenio de Budapest sin reservas ni modificaciones y depositó el instrumento de adhesión en marzo del 2014 ante la Secretaría del Consejo de Europa, convirtiéndose así en el segundo país latinoamericano en ratificar el Convenio de Budapest, después de la República Dominicana.

Desde la fecha de su ratificación, se han introducido 3 iniciativas legislativas ante la Asamblea Nacional para la adecuación de la normativa legal vigente en materia penal a lo preceptuado en el Convenio sobre Ciberdelincuencia de Budapest. El primer anteproyecto legislativo fue presentado en 2013, seguido de uno en el año 2014 y, el último y más reciente proyecto, en el mes de septiembre del 2017.

---

1 CSIRT-Panamá. https://cert.pa/

2 Presidente de la República. Decreto Ejecutivo No. 709 de 26 de septiembre de 2011, por el cual se crea el “CSIRT PANAMÁ”. Disponible en: https://cert.pa/wp-content/uploads/2015/09/Decreto-Ejecutivo-no-709.pdf

3 Consejo Nacional para la Innovación Gubernamental. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf

Actualmente Panamá no posee un marco jurídico de protección de datos personales, sin embargo, el 9 de febrero de 2017 se presentó el Proyecto de Ley No. 463 de Protección de Datos de Carácter Personal ante la Asamblea Nacional[4], la cual aún está en proceso de discusión en la Comisión correspondiente. Lo cual también es una tarea pendiente para el Estado panameño, ya que la aprobación de un adecuado marco regulatorio en esta materia permitiría una mejor determinación de los bienes jurídicos que se deben proteger en el marco de la legislación sobre ciberdelincuencia.

INICIATIVAS DE LEY SOBRE CIBERDELINCUENCIA.

Es importante destacar que el Código Penal vigente únicamente tipifica 2 conductas como delitos informáticos y no incluye los delitos que se realicen por medios electrónicos, como consecuencia, la adecuación de la normativa penal interna a lo regulado en el Convenio de Budapest es una obligación internacional que Panamá debe cumplir.

En consecuencia, estos proyectos presentados buscan regular dentro de la ley sustantiva de la materia, en este caso a través de reformas al Código Penal, la protección de la información y tipificar las conductas delictivas, relacionadas a la nueva tendencia que incluyen: el acceso ilegal a sistemas informáticos, la suplantación de identidad (pshishing), intercepción ilegal de redes, interferencia, daños en la información (borrado, dañado, alteración o supresión de datos informáticos), extorsiones, fraudes electrónicos, estafas, ataques a sistemas informáticos, calumnia y difamación online, hurtos digitales a bancos, ataques realizados por hackers, computadoras zombies (botnets), violación de los derechos de autor, pornografía infantil, pedofilia, ataques de denegación de servicios, ciberacoso (cyberbullying y cybergrooming), violación de información confidencial, la instalación de software como gusanos, malware, ransomware, spam, entre otros.

La falta de preparación y capacidad adecuada para la investigación criminal de delitos realizados por medios tecnológicos ha generado que Panamá, a través del Ministerio Público, estableciera como mecanismos de investigación y persecución penal en materia de ciberdelincuencia los estándares usuales aplicados a delitos comunes. En otras palabras, elimina el elemento definitivo de un cibercrimen, su característica de medios electrónicos, tecnológicos o de comunicaciones, por el hecho de fiscalizar una actuación común. Sin embargo, esto únicamente puede realizarse en aquellos actuares que constituyen un delito, sin la componenda de su particularidad digital. Como consecuencia, aquellos delitos que se desarrollan en el marco del ciberespacio, por su naturaleza, no pueden ser investigados ni juzgados bajos sus parámetros específicos en Panamá.

4 IPANDETEC. Cronología de un Proyecto de Ley de Protección de Datos de Carácter Personal en Panamá. Disponible en: http://www.ipandetec.org/blog/cronologia-de-un-proyecto-de-ley-de-proteccion-de-datos-de-caracter-personal-en-panama.html

Por ejemplo, en el caso de la captura ilegal de datos bancarios (phishing o pharming) bajo la conceptualización de los verbos rectores del tipo penal, en la actual legislación panameña, no podría ser sancionado el mero hecho de la captura ilegal de los datos personales, se debe esperar a que el delincuente utilice la información obtenida de manera ilegal, para que el Ministerio Público de Panamá tenga la capacidad legal de iniciar el proceso de investigación por el delito.

La reforma que deriva de la implementación del Convenio de Budapest requiere la adecuación del Código Penal así como del Código Procesal Penal. La reforma adecuada de este último permitiría que los mecanismos para la investigación penal aseguren la correcta guía y salvaguarda de los Derechos Humanos y garantías procesales reconocidos por tratados internacionales y la Constitución.

Las modificaciones legislativas presentadas en las iniciativas, únicamente se enfocan en las modalidades de la comisión del delito, en este caso únicamente amplían los tipos penales existentes ejecutados por medio electrónicos. Estos delitos se pueden agrupar conforme al bien jurídico tutelado de la siguiente manera:

- Delitos contra la Libertad e Integridad Sexual,
- Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad,
- Delitos contra la Seguridad Jurídica de los Medios Electrónicos.

Los *delitos contra la Libertad e Integridad sexual* contenidos dentro de los Proyectos responden a lo descrito en el Artículo 9 del Convenio, sobre los delitos relacionados con la pornografía infantil, como parte de los delitos relacionados con el contenido digital.

El conjunto de *delitos contra la seguridad jurídica* de los medios electrónicos se refiere a los Artículos 7 y 8 del Convenio, sobre la falsificación y fraude informático.

Por su parte, el conjunto de artículos referentes a los *delitos contra la inviolabilidad del secreto y el derecho a la intimidad* son, los contenidos en los artículos 2 a 6 del Convenio, como el acceso e interceptación ilícita, ataques a la integridad de los datos y del sistema y abuso de los dispositivos. Los cuales dentro del Convenio se contemplan como los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.

En términos generales, los tres proyectos de Ley presentados hasta el momento, se han enfocado únicamente en modificar la legislación penal sustantiva en el sentido de ampliar a la comisión de las conductas delictivas por medio de las nuevas tecnologías, en algunos casos agregan otras circunstancias agravantes e incorporan nuevos tipos penales.

El Proyecto de Ley 558, que modifica y adiciona artículos al Código Penal, relacionados al Cibercrimen, presentado el 27 de septiembre de 2017, es el que se encuentra más avanzado en la Asamblea Nacional. Sin embargo, carece de una adecuación integral, ya que debería incluir la adopción de nuevos tipos penales más allá de una simple adecuación de tipos penales ya existentes en un entorno cibernético, repercutirá en la lucha contra la ciberdelincuencia en el país. En materia procesal, este proyecto únicamente incluye un apartado sobre la evidencia digital, sin embargo, no profundiza en otros aspectos procedimentales regulados en el Convenio de Budapest.

Las tres iniciativas de reforma al Código Penal que se han presentado como consecuencia de la implementación del Convenio de Budapest, se enfocan principalmente en la regulación de los tipos penales con aspectos electrónicos y han dejado atrás, las reformas en materia procesal; con excepción de una que si hace referencia a la evidencia digital. Esto último dificultaría la adecuada implementación a nivel nacional e internacional de los mecanismos de investigación de ciberdelincuencia, así como el procesamiento de las personas involucradas en estos actos.

CONCLUSIONES

Uno de los principales problemas en el proceso de implementación del Convenio de Budapest en el marco jurídico interno, es la falta de inclusión de los aspectos procesales contenidos en el texto del Convenio (solamente un proyecto contempla reformas en materia procesal). Como consecuencia, esto está causando una aspereza con la Secretaría del Convenio en el Consejo de Europa, ya que consideran que una implementación sin los debidos procedimientos, implican un incumplimiento parcial a las obligaciones internacionales adquiridas por el Estado panameño.

Las 3 iniciativas de reforma al Código Penal presentadas en la Asamblea Nacional tuvieron una terminación prematura, por falta de comprensión de la ciudadanía y del apoyo de los medios de comunicación en el país. Además, la falta de compromiso por parte del Ministerio Público frente a campañas de concientización en materia de los riesgos y delitos cibernéticos, que en algún momento hubieran propiciado en crear espacios de diálogo alrededor de la importancia de la existencia de un adecuado marco normativo en materia de ciberdelincuencia.

La necesidad de estándares legales claros para el proceso de investigación de ciberdelitos, la falta de capacidades adecuadas en las diferentes instituciones públicas que participan en los procesos de persecución penal, dificultan los procedimientos internos para la investigación en ciberdelincuencia.

La construcción de políticas públicas y legislaciones, sustantivas y procesales,

adecuadas a los estándares internacionales en materia de ciberdelincuencia es una urgencia en Panamá. Las entidades públicas que participan en los procesos de investigación penal y de otros sectores, como el sector privado y la comunidad técnica, deben buscar el desarrollo de capacidades para hacer frente en la lucha contra la ciberdelincuencia.

BIBLIOGRAFÍA.

Asamblea Nacional. Código Penal de la República de Panamá, Ley No. 14 de 18 de mayo de 2007.

Asamblea Nacional. Código Procesal Penal de la República de Panamá, Ley No. 63 de 28 de agosto de 2008.

Asamblea Nacional. Constitución Política de la República de Panamá.

Asamblea Nacional. Proyecto de Ley 463, de Protección de Datos de Carácter Personal. Disponible en: http://www.asamblea.gob.pa/proyley/2017_P_463.pdf

Asamblea Nacional. Proyecto de Ley 558, que modifica y adiciona artículos al Código Penal, relacionados al Cibercrimen. Disponible en: http://www.asamblea.gob.pa/proyley/2017_P_558.pdf

Consejo de Europa. Convenio sobre la Ciberdelincuencia. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo Nacional para la Innovación Gubernamental. Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas. Disponible en: https://www.gacetaoficial.gob.pa/pdfTemp/27289_A/GacetaNo_27289a_20130517.pdf

IPANDETEC. Cronología de un Proyecto de Ley de Protección de Datos de Carácter Personal en Panamá. Disponible en: http://www.ipandetec.org/blog/cronologia-de-un-proyecto-de-ley-de-proteccion-de-datos-de-caracter-personal-en-panama.html

IPANDETEC. IPANDETEC promueve creación de Sub-comisión para la discusión de Proyecto de Ley de Protección de Datos Personales. Disponible en: http://www.ipandetec.org/blog/ipandetec-promueve-discusion-de-proyecto-de-ley-de-proteccion-de-datos-personales.html

Presidente de la República. Decreto Ejecutivo No. 709 de 26 de septiembre de 2011, por el cual se crea el “CSIRT PANAMÁ”. Disponible en: https://cert.pa/wp-content/uploads/2015/09/Decreto-Ejecutivo-no-709.pdf

IPANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

@ | DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina