Revista Científica Orbis Cognita
Año 4 – Vol. 4 No. 1 pp. 113-134 ISSN: L2644-3813
Enero – Junio 2020
Recibido: 18/10/2019; Aceptado: 5/1/2020; Publicado: 15/1/2020

Regulaciones panameñas a los delitos informáticos que afectan los Sistemas de Información Contables Administrativos (SICA)

Panamanian Regulations related to the Cybercrimes that affect the System of Information accountants administrative (SICA)

José R. Godoy T.
Universidad de Panamá, Centro Regional Universitario de San Miguelito
renegodoy10@gmail.com

RESUMEN

Los grandes avances tecnológicos, la característica intrínseca del Internet, (inexistencia de fronteras), y el aumento de usuarios inexpertos, se han convertido en el principal campo de acción de cibercriminales que están al asecho para crear novedosas y complejas formas de infringir la ley. A su vez, estos adelantos, que han contribuido a lo que hoy conocemos como "Globalización" han jugado un papel trascendental en el crecimiento económico del mundo, ya que conllevan un sinnúmero de ventajas y desventajas, que han sido de provecho a usuarios y organizaciones. Su creciente vínculo, traspasa las fronteras de los países creando espacios suficientes a diferentes ámbitos de la vida, sociedad, negocios diversos, entre otros. Por otro lado, la mencionada inexistencia de fronteras, ofrece un mayor número de oportunidades a cibercriminales de perpetrar diferentes actos o comportamientos antisociales, principalmente agresiones mal intencionadas a sistemas de información. Estos hechos han motivado a los gobiernos, a hacer frente a tales circunstancias aportando respuestas expeditas que faciliten la protección de los usuarios, tanto empresas como particulares, a través de regulaciones las cuales desde hace mucho tiempo se han tratado de unificar para que exista una misma normativa a todos los países. En 2001 el consejo europeo asumió este reto, tratando así de mitigar el problema de la supranacionalidad, pero de acuerdo al estudio exhaustivo por la ONU en 2013, el verdadero foco del problema son los países menos desarrollados, pues estos son los mayormente vulnerables al cibercrimen.Es de aquí donde surge el objetivo e interés de este artículo, investigar cuales son las regulaciones o normativas existentes en Panamá, que pueden controlar, prevenir o mitigar esta problemática latente a nivel mundial que puedan afectar específicamente a los Sistemas de Información

Contables y Administrativos y por ende las organizaciones y usuarios que utilicen los mismos.

PALABRAS CLAVE regulaciones, delitos, Sistemas de Información Contables Administrativos (SICA).

ABSTRACT

The great technological innovations, the intrinsic characteristic of Internet, and the increase of inexperienced users, have become the main field of action of the cybercriminals, who are on the lookout to design novel and forms of infraction of the law. In turn, these innovations, which have contributed to what today is well was known as "Globalization", has played a transcendental role in the world's economic growth and has been without a number of advantages and disadvantages that have worked of benefit and users and organizations. Their growing bond, crosses the borders of countries. On the other hand, the aforementioned non-existence of borders offers a bigger number of opportunities to perpetrate different acts or antisocial behavior, mainly malicious attacks on information systems. These facts have motivated governments to confront history, people, and companies. Regulations to all countries. In 2001, the European Council took on this challenge, trying to mitigate the problem of supranationalism, but according to the UN's comprehensive study in 2013, the real focus of the problem are the least important countries, as these are mostly vulnerable to cybercrime. This is the objective of our investigation since Panama, a developing country and in regard to this type of acts, may suffer damages, to the electronic banking operations and the organizations and users that manage this type of service. This is where the objective and interest of this article arises, to investigate what are the existing regulations in Panama that help control, prevent or mitigate this problem latent worldwide that may specifically affect the Accounting and Administrative Information Systems and therefore the organizations and users that manage them.

KEYWORDS regulations, crimes, Administrative Accounting Information Systems.

INTRODUCCIÓN

En este trabajo, se presenta una revisión de la problemática existente, partiendo de su definición, las diferentes motivaciones por las cuales se da este fenómeno, sus características, además, abordaremos, aspectos principales de la problemática para hacer cumplir las leyes tanto en el plano nacional, como internacional, debido a la mencionada inexistencia de

fronteras, lo cual dificulta la puesta en marcha de mecanismos de prevención y control que ayuden a mitigar este flagelo. También, se definen los Sistemas de Información Contables Administrativos y se presentan datos estadísticos de cómo estos son afectados por los delitos informáticos. Concluimos con algunas observaciones que han de contribuir a una mejora tanto en el plano penal como procesal penal, así como de integración entre países y la adecuada capacitación que deben tener las autoridades a cargo de las investigaciones.

DESARROLLO

Para Carlos Sarzana, citado por Estrada (2006) en su obra Criminalista e Tecnología, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo" (p.4).

Las motivaciones y variedades de actos criminales a nivel mundial son muy diversas, en cuanto al orden cibernético, podemos encontrar, los que están relacionados al contenido informático, intereses financieros, atentados contra la confidencialidad, integridad y accesibilidad a sistemas informáticos.

Hay que mencionar, además que en cuanto a la amenaza y riesgo relativos también son vistos de forma distinta por gobiernos y empresas privadas, lo que dificulta la realización de comparaciones estadísticas entre países, ya que los datos manejados por la policía no simbolizan base sólida para elaborar las mismas.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODOC),manifestó que los países participantes del Grupo de expertos encargado de realizar el estudio exhaustivo sobre el delito cibernético celebrado en Viena del 25 al 28 de febrero de 2013, expresaron que sus sistemas policiales son deficientes para registrar los delitos informáticos, por lo que puede existir una disparidad ya que los datos policiales se ven afectados por factores como los niveles de desarrollo de un país y la capacidad policial especializada en esta área, más que con las tasas de delincuencia existentes.

Además, señala este estudio que:

> En 2011 al menos 2.300 millones de personas, equivalente a más de un tercio de la población total del mundo, tuvo acceso a Internet. Más del 60% de todos los usuarios están en los países en desarrollo y el 45% de todos los usuarios de Internet tienen menos de 25 años. Se estima que para 2017 las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70% de la población mundial. Para 2020 el número de dispositivos interconectados por la red ("Internet de las cosas") será seis veces mayor al número de personas, lo que transformará la concepción actual de Internet. En el mundo hiperconectado del futuro será difícil no imaginar un "delito informático", o quizás ningún delito, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo Internet (p.3).

Por el contrario, las encuestas de victimización, para este estudio exhaustivo, son consideradas como base sólida para realizar comparaciones, es así como se demuestra que la victimización individual es considerablemente superior a otras formas de delitos convencionales, además señala algunos datos o tasas porcentuales de victimización de algunos delitos informáticos (2013):

> Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a una tentativa de "pesca de datos" o "phishing", o sufrir el acceso no autorizado al correo electrónico varían entre el 1% y el 17% de la población con acceso a Internet de 21 países

> de todo el mundo, mientras que las tasas de delitos típicos, como robo, hurto y robo de coches, son en esos mismos países inferiores al 5%. Las tasas de victimización en el caso de delitos cibernéticos son más altas en los países con menores niveles de desarrollo, lo que indica la necesidad de aumentar las medidas de prevención en esos países (p.3).

Luego, en su apartado intitulado ***panorama mundial del delito cibernético,*** se indica que:

> Los funcionarios encargados de hacer cumplir la ley que respondieron al estudio consideraron que a nivel mundial habían aumentado los actos de delito cibernético a medida que tanto personas como los grupos delictivos organizados buscaban nuevas posibilidades ilícitas para obtener ganancias y beneficios personales. Se estima que más del 80% de esos actos tienen su origen en alguna forma de actividad organizada, con mercados negros cibernéticos establecidos en un círculo de creación de programas informáticos maliciosos, infección informática, gestión de redes zombi o "botnet", recolección de datos personales y financieros, venta de datos y obtención de dinero a cambio de información financiera. Los delincuentes cibernéticos ya no necesitan pericias ni habilidades técnicas complejas. Especialmente en el contexto de los países en desarrollo han aparecido subculturas de jóvenes dedicados al fraude financiero relacionado con la informática, muchos de los cuales comenzaron a participar en dicho delito en sus últimos años de adolescencia (p.3).

De acuerdo a Temperini (2013) el cual cita uno de los estudios de mayor relevancia mundial en delitos informáticos (*Symantec Corporation, Informe de Norton sobre delitos informáticos para el año 2012*), en el cuál, "se han entrevistado más de 13.000 adultos en 24 países, para el año 2012, se calculó que los costos directos asociados con los delitos informáticos que afectan a los consumidores en el mundo ascendieron a US$ 110.000 billones en doce meses" (párr. 5).

El mismo estudio revela que, "por cada segundo, 18 adultos son víctimas de un delito informático, lo que da como resultado más de un millón y medio de víctimas de delitos informáticos cada día, a nivel mundial" (párr.5).

Sin embargo, un factor muy importante y en el que desde hace mucho tiempo se hace énfasis, es que las fronteras de los países constituyen un incuestionable obstáculo para la detección, investigación, persecución y castigo de los autores de delitos perpetrados mediante el uso de estas nuevas tecnologías, en contraste con Internet, la cual está configurada como un espacio sin fronteras para aquellos, por lo que señala Gómez (2010) "La dimensión supranacional juega, por tanto, una importancia crucial en el tratamiento de los delitos informáticos. Es imperativa la ejecución de políticas conjuntas, generales, que integren a todos los Estados y sectores de la sociedad" (p.183).

De ahí que, podemos apreciar en primera instancia, algunas características de los delitos informáticos, entre estas, suponen actividades criminales con el uso de las Tecnologías de la Información y Comunicación (TIC´S), se dan por diversos motivos y a través de formas variadas, son vistos de manera distinta por gobiernos y la empresa privada, hecho este que dificulta la comparación estadística entre países, y el problema transfronterizo. Además, que los países, a falta de ejecución de políticas conjuntas, en el plano del Derecho, clasifican los delitos en mención, como hechos típicos o comunes, de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., propiciando la creación de nuevas posibilidades para el uso indebido de las computadoras.

Algunas definiciones propuestas por diferentes autores:

Señalan los expertos, en el nivel internacional, que, pese a los muchos esfuerzos por dar una definición propia con carácter universal para el delito informático, no se ha encontrado la misma, sin embargo, se han formulado conceptos prácticos en función de las realidades existentes en cada país.

Dicho lo anterior, y tomando como referencia algunas definiciones que se han intentado dar en México, cabe destacarla de Julio Téllez Valdés, la cual señala que:

> No es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de 'delitos' en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión 'delitos informáticos' esté consignada en los códigos penales, lo cual, en nuestro país, al igual que en otros muchos, no ha sido objeto de tipificación aún (p.187).

Valdés (2008) conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin", y por las segundas, "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (p.187).

En nuestra consideración los delitos informáticos son: "conductas o actitudes ilícitas, que van en contra de la Ley, y en la que están involucrados el uso de equipos computacionales con el fin primordial de generar lucro y daños a la propiedad física como personal".

En cuanto a los Sistemas de Información, señala Cohen & Asín (2009) "Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio" (p.4).

Por otro lado, Catacora (1997) "Un sistema es un conjunto de elementos, entidades o componentes que se caracterizan por ciertos atributos identificables que tienen relación entre sí, y que funcionan para lograr un objetivo común" (p.25).

Además, Paz (2015) "En la actualidad, los avances tecnológicos han aportado su grano de arena en el mejoramiento de la información financiera, permitiendo obtenerla en el momento

deseado, o sea, justo a tiempo (JAT)" […]" Estos avances han satisfecho la necesidad de anotar las transacciones y los registros contables que otrora se hicieran rudimentariamente" […]" dando como resultado que la contabilidad de hoy se conozca como el lenguaje moderno de los negocios" (p.2).

Otros autores amplían sobre el tema:

En cuanto a este, indica Rúa (2006) "El conocimiento y la innovación tecnológica juegan un papel capital en las actividades económicas y en el desarrollo de las naciones" (p.35).

Además, Alfaro (2008) manifiesta que, la técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen, lo que resulta más dramático en las sociedades informatizadas, en la medida que éstas resulten tecnológicamente vulnerables (p.125).

Amplia, Concepción (2014): "afortunadamente el Derecho Penal y el Derecho Procesal Penal han evolucionado para enfrentarse a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico, diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los principios vigentes" (p.211).

Morales et al (2017) señala que:

> el uso y manipulación fraudulenta de los computadores para destruir programas o datos así como el acceso y uso indebido de información que afecte la privacidad son considerados como medios relacionados con el procesamiento electrónico de datos con el que se puede dar la posibilidad de obtener un gran provecho económico así como también causar considerables daños materiales o morales, tomando en consideración la basta cantidad de datos o información que los sistemas informáticos nos pueden ofrecer sobre actividades bancarias, financieras, tributarias y personales (p.109).

Dicho lo anterior Rayón et al. (2014) señala que “para hacer frente a esta forma de delincuencia se precisa realizar un enfoque supranacional, con unidades policiales de investigación especializadas y dotadas de los medios técnicos necesarios para la efectividad de su trabajo e, igualmente, se hace preciso un enjuiciamiento rápido y especializado de este tipo de conductas (p.212).

Morales (2017) “el peligro real de la humanidad radica en la posibilidad de que individuos o grupos sin escrúpulos aspiren al poder que la información puede conferirles, sea utilizada en la satisfacción de sus propios intereses en franca violación a los derechos y libertades individuales en evidente daño a los individuos de una sociedad” (p.109).

Como se podrá apreciar cada uno de los autores señalados con anterioridad conceptualizan o definen el delito informático de manera que todas conducen a un mismo concepto, son actos criminales perpetrados con el apoyo de la informática o de técnicas modernas anexas.

Algunas regulaciones en el plano internacional y la problemática para hacer cumplir las mismas.

Como mencionamos de inicio, la proliferación del Internet se da a ritmo conmocionado, el uso de este se ha convertido en muchos países en el día a día, pues ha llegado a más hogares y cada vez más personas aprenden a utilizarlo de la mano delas nuevas Tecnologías de la Información y Comunicación (TIC´S).

De igual manera sucede en países subdesarrollados, en los que se crean verdaderos «paraísos cibernéticos», donde se promueven el vacío legal con el fin oportunista de captar beneficios que en otras jurisdicciones resultan ilegales.

Señala Gómez (2010) que: "Internet es un fenómeno relativamente reciente; su aparición se enmarca en la segunda mitad del siglo XX y su utilización a gran escala en los inicios del actual. Es quizás por este motivo que todavía hoy carece de pautas fijas de acción, de normativa capaz de responder a la mayor parte de los problemas que se plantean" (p.178).

En otras palabras, la ausencia de autoridad alguna, que controle y regule Internet, hace que se compliquen aún más los problemas. De ahí que podamos afirmar que las regulaciones de las nuevas tecnologías y en especial de Internet van a estar siempre en un constante vacío, que será cubierto paulatinamente mediante la autorregulación, a no ser que, exista norma positiva que establezca una visión de cierta seguridad jurídica. Y todo es debido a que el Internet evoluciona, avanza a gran velocidad, se transforma, siempre está en constante desarrollo y crecimiento.

Otro factor de mucha afectación que colabora a acrecentar dicha problemática es el tratamiento que se le da a los delitos informáticos, el cual es planteado por los diferentes países en el plano nacional o por vía de tratados multilaterales, siendo actualmente el principal referente el conocido Tratado Europeo o de Budapest, el cual es considerado tanto en materia de Derecho Informático como de cooperación internacional en general, como líder indiscutible de las nuevas formas de asistencia entre Estados. Este se crea con la aspiración común de las partes en llegar a homologar resultados sobre la forma adecuada con

la que se deben procesar diferentes fenómenos, y aunque sólo regula un limitado número de países y en el fondo no menciona de forma explícita en particular los delitos informáticos, como viene diciendo Rodríguez Bernal, puede ofrecer marco jurídico suficiente para regular dicho fenómeno.

Es así como por medio de acciones conjuntas, decisiones, convenios de cooperación policial y judicial, etc., el Consejo Europeo, puede controlar una parte importante en este asunto, suministrando herramientas que sirvan para dar seguimiento y que influyen casi directamente a los delitos informáticos.

Sabemos que en aspectos de cooperación resulta complicado lograr una coincidencia entre países, ya que estos poseen particularidades e intereses diferentes, así como también, la herramienta antes descrita no solucionará todos los problemas que se presenten; a pesar de todo, la solidaridad entre culturas, así como la afluencia e intercambio conjunto de ideas y soluciones es su principal ventaja en la corrección de muchas de sus dificultades.

Dicho lo anterior, queda clara la importancia en el ámbito de la cooperación internacional en vías de la persecución de los delitos informáticos; por lo que nos queda la tarea de romper las barreras ante la disparidad diplomática de los países y forzar a los Estados a tomar decisiones conjuntas para resolver los problemas que les afectan.

Regulaciones en el plano nacional, Panamá y su problemática.

Nuestro país no escapa de la realidad mundial de la globalización y mucho menos de la disparidad del gobierno en cuanto a la atención que debe prestarse a este fenómeno, cada día

aumentan más los avances tecnológicos y por ende la comisión de nuevas conductas delictivas, las cuales no pueden ser atendidas por la carencia de leyes acordes a estas, por lo que se hace necesario, de manera expedita, un cambio de perspectiva, una ruptura a esa burocracia que logra es entorpecer el desarrollo de herramientas que ayuden a encausar estos.

Señala Rojas Parra (2016),

> 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 (p.222).

Factores como las categorías inadecuadas de los tipos penales que van de la mano con las exigencias de la gran demanda de nuevas conductas que no se encuentran reglamentadas, traen como consecuencia que no se puede cumplir con el desarrollo de investigaciones dentro de procesos penales, y el logro de imposiciones acordes a dicha conducta, por falta de acciones correctivas, que condenen luego de una investigación. Todavía cabe señalar, los inconvenientes al solicitar colaboración a otros países, debido a que, en las legislaciones de estos, no se encuentren regulados estos tipos penales.

Dicho lo anterior, presentamos una cronología de las regulaciones de nuestro país en su esfuerzo de controlar y dar solución a este fenómeno.

Panamá, da sus primeros pasos en la búsqueda de mitigar los delitos informáticos, bajo la estructura de la Autoridad Nacional para la Innovación Gubernamental, del Ministerio de la Presidencia, se aprueba el Decreto Ejecutivo No.709 de2011, con el que crea el *Computer Security Incident Response Team*, (CSIRT), con el propósito de prevenir e identificar ataques e incidentes de seguridad a los sistemas informáticos de la infraestructura crítica del país.

Por otro lado, en marzo de 2013, fue aprobado la denominada *Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas*, (por esta misma entidad), la cual establece una serie de acciones para mejorar la ciberseguridad y brindar protección a infraestructuras vitales del país, sin resultados positivos, ya que, la falta de voluntad política, una vez más, obstaculiza su implementación y desarrollo por parte de las entidades encargadas.

Además, en materia internacional, Panamá se adhiere y ratifica al Convenio sobre la Ciberdelincuencia, denominado también como Convenio de Budapest, a través de la Ley 79 del 22 de octubre de 2013, aprobada por la Asamblea Nacional de Panamá, y publicada en la Gaceta Oficial en octubre de ese mismo año, el cual convierte a nuestro país en el segundo en Latinoamérica en estar adherido a este.

En particular, lo que llama a la atención, es que su texto, el cual fue aprobado sin restricciones ni modificaciones y consignado ante la Secretaría de dicho Consejo Europeo, sin embargo, se han presentado tres iniciativas, a la Asamblea Nacional desde la fecha de su ratificación,(2013, 2014 y la más reciente en 2017) con el fin de adaptar la reglamentación legal vigente en materia penal a lo ordenado por dicho convenio, sin resultados satisfactorios,

lo que deja a nuestro país sin cumplir con el compromiso internacional para el cual se adjuntó, ya que como señalamos con anterioridad, nuestro Código Penal vigente solo tipifica dos conductas como delitos informáticos, que no incluyen los que se realicen por medios electrónicos, por lo que se crea un vacío y aumenta la importancia de adecuar la normativa penal interna a lo concertado a este convenio.

Los anteriores conceptos se esclarecerán en lo que sigue, Señala Fratti (2018) que,

> 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 como: Delitos contra la Libertad e Integridad Sexual, Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad y Delitos contra la Seguridad Jurídica de los Medios Electrónicos (p.7).

Amplía, Fratti (2018)

> 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" (p.7) […] 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*** (p.7)**.**

En términos generales, la problemática radica en que, los tres proyectos de Ley presentados hasta el momento, sólo se enfocan en la modificación de la legislación penal sustantiva, orientadas, en ampliar la comisión de las conductas delictivas por medio de las nuevas tecnologías, en algunos casos agregan otras circunstancias agravantes e incorporan nuevos tipos penales, y han dejado atrás, las reformas en materia procesal; con excepción de una que

si hace referencia a la evidencia digital; esto causa grandes dificultades, pues no proporciona una senda para el uso de herramientas, que, a nivel nacional e internacional, ayuden a una investigación ciberdelictual, ni el debido proceso de las personas implicadas en este tipo de crímenes.

Dicho lo anterior, urge la necesaria aprobación de un marco regulatorio en la materia, que permita una mejor precisión de los bienes jurídicos que se deben proteger ante los vastos tentáculos del fenómeno de la ciberdelincuencia.

Como señala Núñez (2017),

> La Procuraduría General de la Nación presentó este miércoles, ante el Pleno de la Asamblea Nacional (AN), el proyecto de Ley "Que modifica y adiciona artículos al Código Penal, relacionados con el Cibercrimen", con el fin de penalizar los delitos concernientes a la seguridad informática para enfrentar las tecnologías utilizadas de forma indebida.[…] A través de un comunicado, el MP (Ministerio Público) detalló que uno de los propósitos del proyecto de ley, es regular la ley sustantiva, la protección de la información, tipificar conductas delictivas, relacionadas a las nuevas tendencias 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 zombis (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. (p.1)

Además, amplia Núñez (2017),

> El proyecto establece normas de tipo procedimental que se adecuan a aspectos y exigencias internacionales, toda vez que el delito va

> modificándose, a través del uso de las redes, de las computadoras, los celulares o de cualquier otro medio digital que sirva para cometer este tipo de situaciones.
> Rodríguez (Procurado de la Nación encargado) aseguró que estas nuevas propuestas se requieren hacer con carácter de urgencia, en virtud de que en la actualidad carecemos en el país, de estos tipos penales que exige la gran demanda de nuevas conductas jurídicas es decir de las penalidades, que no están en la actualidad debidamente reglamentadas.
>
> Es necesario que Panamá cuente con ellas toda vez que así nos adecuamos a las exigencias internacionales y al Convenio de Budapest de 2001, sobre la Ciberdelincuencia del cual somos signatarios, concluyó el Procurador Encargado (p.1).

Llegados a este punto, Panamá no poseía un marco jurídico de protección de datos personales, por lo cual se presentó en febrero de 2017 el Proyecto de Ley No. 463 de Protección de Datos de Carácter Personal ante la Asamblea Nacional, el cual fue aprobado mediante la Ley 81, denominada, Ley Sobre Protección de Datos personales, del 26 de marzo de 2019 y publicada el 29 de marzo de este mismo año en la Gaceta Oficial N°28743-A.

Esta Ley, en su Artículo 1, señala que fue creada con el objetivo de "establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales, de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten datos personales, en los términos previstos en esta Ley". Además, se basa en una serie de principios los cuales fueron los que inspiraron su carácter rector.

Se debe agregar, que otro factor de mucha importancia, es la precaria preparación y capacidad investigativa que poseen las entidades encargadas, ante los cibercrímenes. Al no contar con estas, Panamá, a través del Ministerio Público, dispone mecanismos de investigación y persecución penal en materia de ciberdelincuencia, como estándares usuales aplicados a delitos comunes.

Como señala Fratti (2018),

> Elimina el elemento definitivo de una ciberdelincuencia, 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 (p.6).

Es necesario recalcar, y hacer mención que lo anterior no aplica a aspectos relacionados a la protección de datos personales, ya que la reciente Ley, que trata al respecto, es un avance positivo en materia de regulaciones a delitos informáticos en nuestro país, pues enmarca, todo lo concerniente al debido control y uso en cuanto a los datos de carácter personal; además, tipifica las sanciones y quienes serán las entidades encargadas de dictarlas. Quiere decir esto que, ya no 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.

En síntesis, la legislación panameña, necesita una urgente reforma del Código Penal, al igual que el Código Procesal Penal, para que se estos se puedan adaptar al Convenio de Budapest; teniendo en cuenta que, una adecuada implementación de estos (enfatizando más en el

Código Procesal Penal), facultaría a los mecanismos para la investigación, asegurando la correcta guía y salvaguarda de los Derechos Humanos y las garantías procesales reconocidas por tratados internacionales y la Constitución.

Además de lo antes mencionadas, se presentan también las Leyes y decretos creados en la República de Panamá que se enmarcan en delitos que guardan relación con nuestro objeto de investigación y conexos, las que referimos a continuación:

- Asamblea Nacional de Panamá. Proyecto de Ley No.558. (27 de septiembre de 2017). Que modifica y adiciona artículos al código penal, relacionados con el cibercrimen.

- La Ley 15 de 8 de agosto de 1994 y su Decreto No. 261 de 3 de octubre de 1995, los cuales regulan los derechos de autor y derechos conexos, en su capítulo II, intitulado Programas de Ordenador.

- Ley 43 del 31 de julio de 2001donde se regula lo concerniente a la firma electrónica y los negocios electrónicos.

- Decreto ejecutivo 101 del 17 de mayo de 2005, por el cual se prohíbe el acceso a personas menores de edad a sitios web de contenido pornográfico.

- Ley 14 de 18 de mayo de 2007. Por el que se adiciona artículos al Código Penal relacionados al cibercrimen.

- Ley 51 de 18 de noviembre de 2009, que dicta normas para la conservación, protección, suministro de datos de usuarios de los servicios de telecomunicaciones y su proyecto de Ley 327 de marzo de 2011, que realiza modificaciones y adiciona artículos a la Ley 51 de 2009.

CONCLUSIÓN

Como señalamos con antelación, en nuestro país, se hace de carácter urgente una adecuada reforma a la legislación, en lo que respecta al Código Penal, y al Código Procesal Penal, para que se estos se puedan adecuar al Convenio de Budapest; partiendo del hecho que, de esto

(enfatizando más en el Código Procesal Penal), facultaría adecuados mecanismos para la investigación, asegurando la correcta guía y salvaguarda de los Derechos Humanos y las debidas garantías procesales, constitucionales y reconocidas en tratados internacionales.

Por otro lado, urge también, la necesidad de capacitar a los entes policiales encargados de llevar las investigaciones, toda vez que estos puedan cubrir de forma adecuada, las exigencias técnicas, operativas y logísticas para combatir los delitos informáticos, ya que factores como la supranacionalidad, hace que las fuerzas de seguridad de cada país se encuentren limitadas por sus fronteras lo que dificulta la aplicación de la ley en concreto.

Otro factor de mucha importancia, del cual Panamá no escapa, es que cada país trabaja por separado y sin revelar datos que puedan servir a una investigación en contra de los ciberdelincuentes, los que se colaboran mutuamente para lograr su objetivo, toda vez que, al momento de iniciar una investigación se encuentran dificultades para indagarles, recabar pruebas, retrasos en la negociación de la jurisdicción entre las agencias de investigación, entre otros.

Además, se debe tener presente que para los que perpetran este tipo de delitos, no es de mucha importancia una legislación que los condene, toda vez que su alto conocimiento relativo a la tecnología les permite realizar los crimines desde cualquier parte del mundo sin dejar rastro alguno.

Por lo anterior, se hace imprescindible una adecuada comunicación y colaboración entre países, toda vez que los delitos de este orden van en aumento, la información relacionada a

estas investigaciones se encuentra fragmentada, y las cifras indican que, aunque contemos con un instrumento jurídico internacional que nos sirva como modelo o guía a los países para legislar en materia de ciberdelincuencia, encontramos que las leyes no son capaces de mitigar las cifras de estos.

Y es que los países, en su intento de regular estos, describen específicamente un delito informático, lo cual hace que la norma prontamente quede desfasada, por lo que, para evitar sucumbir en estas situaciones, es imprescindible que se realicen las investigaciones que contribuyan a profundizar en la naturaleza del problema y con la característica transnacional del mismo.

Por lo que, sin lugar a duda, se da la urgente necesidad, en nuestro país y el mundo, de una solución integral, seria, armónica entre los distintos países, que asegure la cooperación internacional, como arma para combatir la delincuencia informática.

REFERENCIA BIBLIOGRÁFICA

Alfaro, L. (2002). Los Delitos Informáticos – Aspectos Criminológicos, Dogmáticos y de Política Criminal, JURISTA Editores E.I.R.L. Lima. pág.125

Catacora. F. (1997). Sistemas y Procedimientos Contables. McGraw-Hill-Interamericana de Venezuela, S. A. Venezuela.

Cohen & Asín. (2009). Tecnologías de Información en los Negocios. Quinta Edición McGRaw-Hill/Interamericana Editores, S. A. DE C. V. México.

Concepción, M. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, XLVII (2014) 209-234. España.

Oficina de las Naciones Unidas contra la Droga y el Crimen **(UNODOC)**. (2013). Estudio exhaustivo sobre el delito cibernético. Nueva York.

Estrada, M. (2006). Delitos Informáticos. Universidad abierta. México.

Gómez, A. (2010). El delito informático su problemática y la cooperación internacional como paradigma de su solución: el Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR). p. 183

Paz, N. (2015). Contabilidad General. Quinta Edición. McGraw-Hill Interamericana. 2015.

Rayón et al. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Universidad Complutense de Madrid.

Rúa Ceballos, N. (2006). La Globalización del conocimiento científico-tecnológico y su impacto sobre la innovación en los países menos desarrollados. Revista Tecno Lógicas. Colombia. P.35-57.

Morales, C. y otros. (2017). Delitos informáticos en el Estado de Guerrero. Universidad Autónoma de Guerrero. México.

Temperini, M. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.

Leyes y decretos

Asamblea Nacional de Panamá. Proyecto de Ley No.558. (De 27 de septiembre de 2017). Que modifica y adiciona artículos al código penal, relacionados con el cibercrimen.

Ley 15 de 8 de agosto de 1994. Derechos de Autor y Derechos Conexos. Capítulo II, Programas de Ordenador.

Ley 43 del 31 de julio de 2001. El cual regula lo concerniente a las Firmas y comercio electrónicos.

Decreto ejecutivo 101 del 17 de mayo de 2005. Por el cual se prohíbe el acceso a personas menores de edad a sitios web de contenido pornográfico (Gaceta Oficial No. 25.311 de 17 de mayo de 2005).

Ley 14 de 18 de mayo de 2007. Por el que se adiciona artículos al Código Penal relacionados al Cibercrimen.

Ley 51 de 18 de noviembre de 2009. Por la cual se dictan normas para la conservación, protección y el suministro de datos de usuarios de los servicios de telecomunicaciones. (Gaceta Oficial No. 26.374 de 23 de septiembre de 2009).

Proyecto de Ley 327 de marzo de 2011. Que modifica y adiciona artículos a la Ley 51 de 2009, que dicta normas para la conservación, protección y el suministro de datos de usuarios de servicios de telecomunicaciones.

Ley 81del martes 26 de marzo de 2019. Sobre Protección de Datos Personales. (Gaceta Oficial No. 28743-A de 29 de marzo de 2019).

Infografía

Astudillo, M. (2008).Consideraciones para la selección de sistemas de información Contables y Administrativos en la pyme colombiana. Entramado, vol. 4, núm. 2, julio-diciembre, 2008, pp. 52-69. Consultado el: 16 de septiembre de 2019. Recolectado de: file:///E:/CONGRESO-SEMINARIO/artículo_redalyc_265420459005.pdf

Fratti, S. (2018). Panamá: Un País con la necesidad de una legislación sobre Cibercrimen. Ipandetec-Instituto Panameño de Derecho y Nuevas Tecnologías. Consultado el: 15 de septiembre de 2019. Recolectado de: https://www.ipandetec.org/wp-content/uploads/2018/08/IPANDETEC-Budapest-final-DD.pdf

Núñez, O. (2017).Presentan proyecto de ley que busca penalizar delitos cibernéticos en Panamá. Telemetro.com/Nacionales. Consultado el: 29 de agosto de 2019. Recolectado de: http://www.telemetro.com/nacionales/Presentan-Codigo-Penal-relacionados-Cibercrimen_0_1066994305.html

Rojas-Parra, J (2016). Análisis de la penalización del cibercrimen en países de habla hispana. Revista LOGOS CIENCIA & TECNOLOGÍA. Vol. 8. (No. 1), [221,222]. ISSN 2145–549X | ISSN 2422-4200. Consultado el: 16 de agosto de 2019. Recuperado de: https://www.redalyc.org/pdf/5177/517754055021.pdf

Traductor de Google. https://www.google.com/search?q=traductor+de+google&rlz=1C1CHNY_esPA703PA703&oq=traductor+de+&aqs=chrome.1.69i57j0l5.4502j0j7&sourceid=chrome&ie=UTF-8

WordReference.com. Diccionario de Sinónimos. http://www.wordreference.com/sinonimos/