LA CIBERDELINCUENCIA EN PANAMÁ Y EL CONVENIO DE BUDAPEST DE 2001.

Especial atención al Proyecto de Ley 632 de 2021

Beermann Hemmerling, Kurt.Universidad de Panamá,
Facultad de Derecho y Ciencias Políticas,
Departamento de Ciencias Penales y Criminológicas, Panamá

RESUMEN

La ciberdelincuencia puede ser contemplada como la conjunción de 2 materias que se encuentran en constante evolución, el derecho (específicamente el derecho penal) y la tecnología, razón por la cual su estudio y tipificación debe ser igualmente dinámico y en constante evolución, ya porque existe una delgada línea que separa el uso correcto de los equipos o sistemas informáticos de los abusos que se comenten con estos o contra estos, así como la facilidad que el mundo virtual ofrece para ejecutar acciones ilícitas de una forma más rápida e incluso cómoda y eficiente.

Es por tal motivo que vemos prudente crear un estudio paralizado entre el Convenio de Budapest de 2001 y nuestro Código Penal en materia de Ciberdelincuencia, no solo para ofrecer de una manera sintetizada y esquematizada estas actualizaciones al lector, sino también ofrecer una plataforma de análisis en cuanto a las mejoras que en materia jurídica tenemos al respecto.

Por último, hacemos referencia al proyecto de Ley 632 de 2021 el cual propone cambios y reestructuración, desde nuestro punto de vista adecuados y necesarios, de cara a fomentar en el lector un carácter crítico de promotor de este proyecto ley el cual estamos completamente seguros de que traerá muchos beneficios a nuestra legislación penal en materia de ciberdelincuencia.

PALABRAS CLAVES: Ciberdelito, ciber-delincuencia, delitos informáticos, sistema informático, datos, equipos informáticos.

KEYWORDS: Cybercrime, cyber-delinquency, computer crimes, computer system, data, computer equipment.

ABSTRACT

Cybercrime could be seen as the convergence of two constantly evolving fields: law (specifically criminal law) and technology. Therefore, the study and classification of these must be equally dynamic and continually evolving. This is because there is a thin line that separates the proper use of computer systems from the abuses committed with or against them. Additionally, the virtual world provides an easy and efficient platform for executing illicit actions more quickly and conveniently.

For this reason, we find it prudent to establish a parallel study between the Budapest Convention from 2001 and our Criminal Law regarding Cybercrime, not just to mention these updates to the reader in a synthesized and structured manner but also to provide a platform for analysis regarding the legal improvements in this area.

Finally, we refer to law project 632 from 2021, which proposes changes and restructuring that, from our point of view are appropriate and necessary. This is aimed at fostering a critical and supportive stance toward this legislative project, which we are completely confident will bring many benefits to our criminal legislation in the field of cybercrime.

SUMARIO: 1. Introducción, 2. Adecuación de la legislación panameña vigente con relación al convenio de Budapest del 2001 sobre ciberdelincuencia, 3. Proyecto de Ley 632 de 2021, 4. Conclusiones 5.Bibliografía

1. Introducción

Hablar de tecnología y avances tecnológicos siempre será un reto en el cual la constante demanda de actualización y estudio representará el mayor reto de todos, y es que el mundo digital crece a una velocidad difícilmente calculable, lo que ayer era extremadamente novedoso hoy es suplantado por nuevas creaciones cada vez más sorprendentes que lo anterior.

Panamá se integra cada vez más al mundo tecnológico, desde la cultura del *smartphone* hasta la infraestructura informática, tanto gubernamental como privada, los panameños hacen a la tecnología cada vez más parte de su vida, de su día a día.

Como todo fenómeno social, el Derecho aparece como un ente regulador de conductas y relaciones entre personas, ya que los mencionados avances tecnológicos forman parte de ese propio fenómeno social, en mayor o menos escala; como muestra podemos mencionar como la utilización de las Inteligencias Artificiales (AI por sus siglas en inglés) trae consigo una serie de situaciones que afectan temas de derechos de autor, plagio, suplantación de identidad, así como cualquier otro en donde quienes hacen uso de ella pueden sacar un provecho pero en detrimento de un derecho ajeno.

De igual forma tanto el delincuente común como el crimen organizado han sido participe de la corriente globalizadora de la última década, y ha encontrado en la tecnología un aliado imprescindible para realizar y coordinar actos delictivos que en gran medida se planifican en un país, pero se desarrollan materialmente en otro. He aquí la importancia de conocer los

mecanismos que posee el Estado (o los Estados), tanto desde el punto de vista de prevención como de la investigación, una vez cometido el ilícito.

No es casualidad que algunos Estados estén inclinándose al uso del Derecho Penal como un instrumento de control social para estas conductas, que se vienen dando cada vez en mayor cantidad, y que lesionan intereses personales o particulares en la llamada *red*.

Panamá, ya en octubre de 2013 que mediante Ley 79 del mismo año, ratifica el Convenio Sobre La Ciberdelincuencia, realizado en Budapest el 23 de noviembre de 2001, adecuando así su legislación penal incorporando tipos que permiten a los jueces y magistrado penalizar hechos perpetrados mediante el uso de equipos electrónicos, o en donde el equipo electrónico es el objeto material (incluso llegando a causar un daño sobre el propio equipo) o en la información contenida en él.

Al realizar una revisión de los artículos que se incorporan en nuestra codificación patria relacionada a lo que, el propio cuerpo normativo ha denominado *"Delitos contra la Seguridad Informática"*, somos del criterio que la incorporación de acciones individuales e independientes, sobre todo en la redacción del artículo 290 vulnera no solo el principio de taxatividad del Derecho Penal, sino también aspectos que puedan perjudicar una adecuada política criminal, y proporcionalidad de la consecuencia jurídica de cada una de estas figuras.

Siendo la tecnología y la informática materias ajenas al Derecho, nos proponemos como punto de partida desarrollar el concepto de nuestro objeto de estudio, los equipos o aparatos electrónicos, en un ámbito general, así como la información contenida en éstos, en un sentido específico.

Tenemos entonces que aparatos electrónicos *"consiste en una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas"* (Wikipedia, Aparato electrónico, 2014). Dentro de estos equipos electrónicos se encuentran los llamados "ordenadores" o como comúnmente se denominan "computadoras", que es el lugar (guardadas proporciones) en donde se almacena la mayor cantidad de información, en un formato digital.

Como mencionamos anteriormente, dentro de estos ordenadores o computadoras se encuentra el segundo objeto del presente estudio, que es la información o los datos, que para la Real Academia de la Lengua Española se define como la *"comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"* (RAE, 2014), y esta tendrá el valor que su dueño le establezca.

La información a la cual hacemos referencia es específicamente la contenida en los equipos electrónicos, sin restricción que estos puedan ser computadores, celulares, servidores, unidades de almacenamiento, etc.

Agregamos, como criterio personal, que la unión entre la primera y la segunda se puede denominar como informática, que para Manuel Ossorio es aquella *"denominación de la*

*técnica informativa basada en el rigor lógico y en la automatización posible, al punto de utilizar con frecuencia, y dentro de las posibilidades, las computadoras (*Ossorio, 1999*)*, es por tal motivo que, en palabras del mexicano Julio Téllez Valdez, los delitos informáticos son aquellas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"*.

Para Arboleda Vallejo/Ruiz Salazar (2001), se "sanciona el acceso ilegal y la utilización indebida de base de datos, red o sistema informático, efectuada tanto por un intruso, como por la persona encargada de la base de datos o sistema informático hecho que puede ser efectuado de manera clandestina, abusiva o ilícita, violando las medidas de seguridad como, por ejemplo, las claves de entrada dispuestas para impedirlo".

Por otro lado, una definición más clara y precisa es plantear a estos como aquellos en donde la acción prohibida (u ordenada) tiene por objeto material un equipo electrónico, o el uso de equipos electrónicos como medios para ejecutar la acción prohibida.

De los primeros podemos mencionar que son los más conocidos y conceptualizados por la doctrina, ya que hablamos de "hechos que atentan contra los elementos físicos del sistema informático (hardware, monitores, dispositivo de almacenamiento de diskettes, cintas, discos, de comunicación etc.) y a elementos lógicos (ficheros, datos y no programas) del sistema informático, es decir, que son hechos que afectan la información almacenada" (Durling, 2009), donde la afectación recae sobre elementos físicos o lógicos del equipo informático.

En cuanto a los segundos hablamos de todas aquellas figuras delictivas en donde el equipo electrónico no es la "materia prima" para la ejecución de la acción, evidentemente puede ejecutarse la acción mediante el uso de estos.

Otro aspecto de importancia para la presente investigación es establecer el bien jurídico tutelado, que son aquellos *"valores significativos para la sociedad organizada."* (Muñoz Pope, 2003), que para gran parte de la doctrina es "la información", criterio que no compartimos, ya que somos de la tesis que estamos frente a un bien jurídico de mayor importancia o extensión como lo es "la confianza de las personas en el uso de los equipos electrónicos", debido a que la primera es uno de los aspectos en cuestión, en tanto que la segunda implica la construcción de un bien inmaterial de tipo plurisubjetivo, es decir que su valor no gira en torno a la consideración de una sola persona, sino a una concepción generalizada sobre el uso o no de estos aparatos tecnológicos que hacen la vida más fácil y rápido.

2. Adecuación de la legislación panameña vigente con relación al convenio de Budapest del 2001 sobre ciberdelincuencia

En reunión sostenida por el Consejo Europeo en noviembre de 2001, el tema de la ciberdelincuencia y/o delitos informáticos forma parte protagónica de la agenda de los estados miembros, debido al alcance que tiene el internet en conductas, que, si bien hasta la fecha no eran consideradas como delitos, era necesario controlar de una forma u otra las mismas, debido a los perjuicios que estas traían.

El llamado convenio de Budapest crea un abanico de figuras delictivas que les servirán a los Estados para adecuar estas a su realidad social particular, situación que nuestro país no supo utilizar esto en su favor, ya que, a nuestro criterio concentró una serie de figuras, a veces incluso contrapuestas, que hacen inaplicable la norma.

Este convenio clasifica, a nuestro criterio de manera acertada, los delitos informáticos bajo 4 títulos, que posteriormente pasaremos a estudiar de forma más amplia, a saber:

- Título 1 sobre Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- Título 2 sobre Delitos Informáticos
- Título 3 sobre Delitos relacionados con el contenido
- Título 4 sobre Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

En la actualidad, Panamá como signatario de dicho convenio, ha tenido que realizar adecuaciones a la normativa penal en esta materia, así tenemos que el Título VIII de Delitos contra la Seguridad Jurídica de los Medios Electrónicos, contiene un Capítulo I sobre Delitos contra la Seguridad Informática, donde establece 2 artículos (289 y 290) con figuras delictivas que básicamente buscan incorporar todas las figuras que el convenio menciona en su llamado Título 1, y 2 artículos (291 y 292) con agravantes relacionadas a la materia o fuente de la información, o bien al sujeto que realiza la acción u omisión.

Estos hacen referencia a los delitos informáticos que denominamos del primer grupo, es decir, los que atentan sobre un equipo informático, ya sea sobre sus partes o información contenida en ellos.

Por otra parte, tenemos aquellos delitos informáticos del segundo grupo, es decir, aquellas en donde el equipo electrónico es un medio o herramienta para la consumación de una figura delictiva independiente, mismos que nuestro código consagra como una modalidad o en otros casos como una agravante de una figura delictiva independiente, incorporando, entre otros, a los delitos que el citado convenio plantea en sus Títulos 2, 3 y 4.

Somos críticos y promotores de una reformulación de nuestra legislación en este tema, sobre todo ubicando todas estas bajo un nuevo apartado, donde se definan claramente cada una de las figuras, que si bien pueden ser similares a otras ya establecidas, la

especialidad de la norma es lo que le daría su validez, y permitiría unirla con una verdadera política criminal, ya que entre otras, erróneamente establece una misma pena para todas las figuras del primer grupo, cuando claramente posee características distintas que hace a unas masa lesivas que a las otras.

Es osado encuadrar todas las figuras delictivas que se pueden ejecutar bajo la óptica de los delitos informáticos del primer grupo, sobre todo la confusa redacción del artículo 290, donde se lesiona gravemente el llamado "principio de taxatividad" que menciona "sólo pueden ser castigadas las acciones u omisiones que expresamente estén descritas como delitos por el legislador, lo que implica tener que definir con precisión el comportamiento prohibido u ordenado" (Muñoz Pope, 2003).

Por tal motivo pasaremos a comparar nuestra legislación penal vigente en materia de ciberdelincuencia en relación con las figuras delictivas propuestas por el convenio de Budapest de 2001 del cual somos signatarios.

A. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Estas figuras delictivas tienen por objeto proteger tanto los equipos electrónicos del sujeto pasivo, como también la información contenida en ellos, bajo 5 figuras que acertadamente cubren, a nuestro criterio, gran parte de las acciones en materia de delitos informáticos de nuestro llamado "primer grupo", dentro de los cuales tenemos:

1. ***Acceso Ilícito***. Figura que el propio convenio define como "el acceso deliberado e ilegítimo a todo o en parte de un sistema informático" (Convenio sobre Ciberdelincuencia, 2001), pero que también debe exigirse el quebrantamiento de una medida o dispositivo de seguridad del equipo electrónico, o la intención de obtener datos informáticos, ya que de lo contrario debemos apegarnos al principio de intervención mínima del derecho penal.
2. ***Interceptación ilícita.*** Toda vez que la gran mayoría de los equipos electrónicos se encuentran interconectados mediante una red privada, o mediante la llamada *"red de redes"* o como comúnmente se denomina *"Internet"*, ya sea mediante el uso de cables de red o mediante ondas (inalámbrico), la información electrónica puede ser captada por otro u otros dispositivos distintos a los legítimamente establecidos. Por tal motivo el citado convenio establece "la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos" (Convenio sobre Ciberdelincuencia, 2001).
3. ***Interferencia en los datos***. Esta figura, a nuestro criterio es una agravante de las figuras predecesoras, toda vez que se establece la penalización de "comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman

datos informáticos" (Convenio sobre Ciberdelincuencia, 2001), toda vez que tanto en el acceso como en la interceptación se puede llegar, con intención o sin ella, a dañar, borrar, deteriorar, alterar o suprimir datos contenido en los equipos electrónicos.

4. **Interferencia en el sistema.** En esta estamos frente al ataque autentico sobre un equipo electrónico, y ya no contra la información que este contenga, toda vez que se penaliza "la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos" (Convenio sobre Ciberdelincuencia, 2001).
5. **Abuso de los dispositivos.** Nuevamente estamos frente a lo que consideramos una agravante aplicable a todas la figuras antes descritas, toda vez que lo que se busca castigar en este artículo es "La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos… una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático" (Convenio sobre Ciberdelincuencia, 2001).

En relación con la primera figura menciona, sobre el acceso ilícito, nuestro código penal establece en su artículo 289 una redacción a nuestro criterio acertada, a saber:

> "Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión"

En cuanto a la segunda, sentimos que el legislador patrio abusó de los recursos gramaticales toda vez que el artículo 290 pretende introducir tanto la interceptación, interferencia y el abuso de equipos informáticos, al establecer:

> "Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión"

De lo anterior se crean 2 situaciones que a nuestro criterio puede subsanarse si se separan estas figuras similares pero independientes entre sí, a saber:

a. Se sancionan con la misma pena a pesar de que uno puede ser más lesivo que el otro, ya que el interceptar la transmisión de un partido de futbol y ponerlo al alcance de otro usuarios que no pagan un determinado derecho de uso es menos perjudicial que

quien interfiera la base de datos del registro público panameño impidiendo el acceso a miles de usuarios, pero ambas figuras tienen la misma sanción.

b. El abuso en las piezas gramaticales puede ocasionar el error, ya del juzgador, del ente investigativo o bien de la defensa técnica a la hora de encuadrar un hecho al tipo penal en cuestión, creando con esto la impunidad.

Por su parte los artículos 291 y 292 establecen agravantes por razones del tipo de información o la calidad del sujeto activo. Tenemos entonces que el 291 un aumento de un tercio a una sexta parte de la pena cuando los datos o sistemas sean de *entidades públicas, autónomas, semiautónomas o de bancos, aseguradoras o demás instituciones financieras o bursátiles*; en tanto que el artículo 292 aumenta la pena entre una sexta y una tercera parte si el sujeto activo es *la persona encargada o responsable de la base o del sistema informático, o la persona autorizada para acceder a este, o las cometió utilizando información privilegiada*.

Ahora bien, erróneamente nuestra legislación penal deja de lado la agravante propuesta en el numeral 3 anteriormente citada, toda vez que no se establece ninguna sanción a quien *borre, deteriore, altere o suprima datos informáticos*; así como tampoco el numeral 5, en donde se evita la creación o comercialización de dispositivos que permitan cometer delitos mediante los propios aparatos electrónicos.

Adicional a los ya mencionados anteriormente, somos del criterio que bajo este apartado también entrarían los delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad cuando se realicen sobre medios tecnológicos o informáticos:

- Inviolabilidad del Secreto y el Derecho a la Intimidad (artículos 164 y 165)
- Divulgación de Comunicación (artículo 166)
- Interceptación de Comunicación (artículo 167)
- Seguimiento, Persecución o Vigilancia (artículo 168)

B. Delitos Informáticos

En este grupo se guarda relación con actividades que tienen por factor común el engaño, toda vez que se habla de la Falsificación y el Fraude informáticos, mismas de las cuales tenemos las siguientes consideraciones:

1. ***Falsificación informática.*** De esta se refiere el citado convenio como "la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles" (Convenio sobre Ciberdelincuencia, 2001).
2. **Fraude informático**. Situación distinta se presenta esta figura, ya que la establecerse para estas "cualquier introducción, alteración, borrado o supresión de datos

> informáticos" o "cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona".

Sobre el primer punto, es importante destacar que actualmente el artículo 366-A, del Capítulo I sobre Falsificación de Documentos en General, que se encuentra en el Título XI sobre Delitos contra la Fe Pública (Código Penal de la República de Panamá, 2007), contempla la *falsificación informática* a quien *indebidamente ingrese, altere, borre, suprima o falsifique datos informáticos, un documento electrónico, un certificado electrónico independientemente de si los datos pueden o no ser leídos directamente o almacenados en un sistema informático o electrónico resultando en datos informáticos no auténticos para que sean adquiridos o utilizados como auténticos con efectos legales*, estableciendo una pena de prisión de cuatro a ocho años.

En cuanto al *fraude informático*, la Estafa contenida en el artículo 220 de nuestro código penal adecua ésta integrando aspectos tecnológicos "cuando se realice a través de un medio cibernético o informático", e incluso la manipulación o alteración de *programas, bases de datos, redes o sistemas informáticos*, de las que habla el Artículo 226, junto a su agravante cuando el sujeto activo sea *la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada*.

C. Delitos relacionados con el contenido

Son los que están directamente relacionados con el flagelo de la pedofilia, toda vez que lo propuesto por el Consejo Europeo es en base a la llamada pornografía infantil, en donde a nuestro criterio se desarrolla de una forma amplia y clara al establecerse en el propio convenio:

> a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
>
> b) la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
>
> c) la difusión o transmisión de pornografía infantil por medio de un sistema informático,
>
> d) la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
>
> e) la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

También otro aspecto importante es que se establece lo que, desde un punto de vista jurídico, se debe considerar como "*pornografía infantil*" al considerar:

> "todo material pornográfico que contenga la representación visual de:
>
> a) Un menor comportándose de una forma sexualmente explícita;
>
> b) una persona que parezca un menor comportándose de una forma sexualmente explícita;
>
> c) imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita."

Por último, se establece también el carácter de "*menor*" a todas las personas que no hayan cumplido 18 años de edad, lo cual es completamente cónsono con nuestro ordenamiento jurídico.

En nuestro código penal se incorpora el tema del que se habla en el convenio de Budapest en el artículo 184 para los puntos **a**, **b** y **c** anteriormente mencionado, al establecer:

> *"Quien **fabrique**, **elabore** por cualquier medio o **produzca** material pornográfico o lo **ofrezca**, comercie, **exhiba**, **publique**, **publicite**, **difunda** o **distribuya** a través de Internet o de 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 diez a quince años.*
>
> *La pena será de quince a veinte 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."*

Es importante resaltar la amplitud, no solo a actos reales sino también simulados, por un lado, y el que se haya establecido una pena mayor por el uso de internet a diferencia de la pena establecida en el tipo base del 179, que establece entre ocho a diez años.

Adicional, el artículo 187 también crea una condición de alcance del Derecho Penal, con relación a pornografía infantil, sancionando a quien "se valga de correo electrónico, redes globales de información o cualquier otro medio de comunicación individual o masiva, para incitar o promover el sexo en línea en personas menores de edad o para ofrecer sus servicios sexuales o hacer que lo simulen por este conducto, por teléfono o personalmente".

En cuanto a los puntos **d** y **e** del convenio, somos del criterio que pueden encuadrar perfectamente en el artículo 185, con la única diferencia, en el caso del punto **e**, que la ley no se centra en la "forma" como se obtuvo el material, sino en el hecho que el sujeto activo lo posea.

> *"Quien **posea** para su propio uso **material pornográfico** que contenga la imagen, **real o simulada**, de personas menores de edad, **voluntariamente adquirido**, será sancionado con pena de prisión de cinco a diez años".*

De lo anterior podemos resaltar el sabio criterio del legislador de conservarlo únicamente en su forma dolosa al incorporar *"voluntariamente adquirido"* ya que pudiese darse el caso que la persona no estuviese buscando tal material pero por una u otra razón se descargó en el equipo electrónico de la persona, o bien fue plantado por otra con más astucia que el imputado; en cualquiera de los casos propuesto lo cierto es que el papel del informático forense será clave para determinar, desde el punto de vista probatorio, cuando estamos ante uno u otro supuesto.

A. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Tal vez el más común y menos perseguido de todos los mencionados anteriormente, la llamada "piratería", que a nuestro criterio obedece totalmente al poder económico que la industria del cine, música y televisión representa, ha llevado a crear una barrera legal para minimizar el impacto que el internet ha causado en las ventas de las industrias antes mencionadas.

Como punto de referencia, el caso Napster iniciado en diciembre de 1999 y finalizado en julio de 2001 marca un hito, a nuestro criterio, en el naciente derecho informático, ya que hasta ese momento estos temas quedaban como casos aislados en la liberalidad que el internet ofrecía. Basado en conexiones P2P (peer to peer) las personas intercambiaban música en un formato de mp3, violando los derechos de los artistas ya que las ventas de discos compactos tuve un bajón considerable.

Misma situación de reciente data se dio mediante el cierre en enero del 2012 de MegaUpload por infracción de derechos de autor debido a que el sitio, creado bajo un esquema de alojamiento de información o datos, mismo que fue utilizado por los propios usuarios para propiciar la descarga de películas, compilaciones musicales, programas "crackeados", entre otros.

Esta última desato, lo que hoy en día se conoce como un auténtico[1] *"terrorismo virtual"* o *"ciber-terrorismo"*, en manos del hoy conocido grupo ***Anonymous*** quienes ganan el mayor protagonismo al *"sacar de línea"*, en señal de protesta, a los sitios web de la NSA[2],

[1] Establecemos "auténtico" ya que en los últimos años se ha pensado, a nuestro criterio erróneamente, que todo acto terrorista en donde sea utilizado un equipo electrónico, especialmente computadores y/o celulares, se está ante un ciber-terrorismo. A nuestro criterio el ciber terrorismo es aquel que se desarrolla completamente en la red y tiene por objeto crear una inestabilidad de la población en uno o más Estados, en los otros casos se está ante un acto terrorista en donde el equipo informático fue el instrumento para llevar a cabo la acción prohibida.

[2] Agencia de Seguridad Nacional de los Estados Unidos, por sus siglas en inglés.

FBI[3] y Sony Music luego que un tribunal norteamericano diera de baja el sitio *MegaUpload*. Situación que tuvo su punto climax con la divulgación de los llamados *Wikileaks*.

Es increíble poder ver como este tipo de actos, que en un momento determinado no son considerados como nocivos o peligrosos, de una forma u otra evolucionan en otros de suma complejidad y que pueden llegar a causar grandes perjuicios a toda una colectividad.

En este aspecto el convenio busca, basándose en convenios y/o acuerdos internacionales como el Acta de París de 24 de julio de 1971, el Convenio de Berna, la Convención de Roma, el Tratado de la OMPI sobre la propiedad intelectual y sobre las obras de los intérpretes y ejecutantes y los fonogramas, específicamente:

- La protección de las obras literarias y artísticas… cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
- La protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión… cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Ya nuestra legislación ha contemplado estos aspectos, específicamente bajo el Capítulo VI sobre Delitos contra la Propiedad Intelectual (Código Penal de la República de Panamá, 2007), dentro de los cuales se encuentra la sección 1 sobre Delitos contra el **Derecho de Autor** y Derechos Conexos de los que podemos mencionar:

> "262. Se impondrá pena de uno a tres años de prisión o de doscientos a cuatrocientos días-multa a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, realice cualesquiera de las siguientes conductas:
>
> 5. Retransmita, por cualquier medio alámbrico o inalámbrico, reproducción y retransmisión de las emisiones de los organismos de radiodifusión de cable o satélite"

Sobre la **Reproducción Ilegal de Emisiones** podemos mencionar que ya existe un precedente reciente en la transmisión del pasado mundial de futbol Brazil 2014 en nuestro país, en donde se da, por lo que conocemos, por primera vez un bloqueo a nivel de direcciones IP de las transmisiones vía web de otros canales internacionales en nuestro país. Tal es el caso, por ejemplo, de la cadena Telemundo Miami, misma que ofrecía a sus televidentes la transmisión gratuita de estos partidos, pero cuando alguien desde Panamá accedía a dicha

[3] Oficina Federal de Investigaciones por sus siglas en inglés.

transmisión recibía un mensaje que "esta transmisión ha sido bloqueada en su país", no así con el otro contenido del sitio web.

Lo anterior lo entendemos como una reacción de los canales de televisión que habían adquirido los costosos derechos de transmisión de los citados partidos, en este caso Televisora Nacional Canal 2 y MEDCOM.

> "266. Quien con fines ilícitos fabrique, ensamble, modifique, importe, venda u ofrezca en venta, arriende o ponga en circulación decodificadores o cualquier otro artefacto, equipo, dispositivo o sistema diseñado exclusivamente para conectar, recibir, eliminar, impedir, desactivar o eludir los dispositivos técnicos que los distribuidores o concesionarios autorizados de las señales portadoras de programas, sonidos, imágenes, datos o cualesquiera combinación de ellos, tengan o hayan instalado, para su protección o recepción, será sancionado con prisión de dos a cuatro años.
>
> Quien en razón de la conducta descrita en este artículo recepte y distribuya la señal portadora de programas, sonidos, imágenes o datos, que fue decodificada sin la autorización del distribuidor o concesionario autorizado, será sancionado con prisión de cuatro a seis años."

Como anteriormente lo habíamos mencionado en la parte introductoria, la evolución de la tecnología va de la mano con las nuevas formas de delincuencia a niveles internacionales, y el artículo anterior no hace sino plasmar aquella situación sobre la cual se ha perdido el control, por ejemplo, con la venta de antenas y decodificadores para tomar señal satelital, que en principio no es ilegal, ya que existen muchos satélites gratuitos o abiertos con los cuales dichas antenas puede funcionar.

La ilicitud en la actividad anterior viene cuando, mediante foros y servidores de otros países, los panameños lograron modificar los decodificadores para que puedan leer la información de los satélites de televisión pagada, claro está, de forma gratuita.

Por último, también el artículo 266-A establece la figura de evasión de controles de acceso (digitales) *con el fin de lograr una ventaja comercial o ganancia financiera privada*, para obtener un acceso a *obra, interpretación, ejecución o fonograma protegido*.

Bajo la Sección 2 sobre Delitos contra los **Derechos de Propiedad Industrial** tenemos una serie de figuras delictivas, de las que anteriormente denominamos "de segundo grupo", es decir que pueden ser cometidas mediante el uso de un equipo electrónico o informático, dentro de la cual a modo de ejemplo podemos mencionar:

> "272. Quien se apodere o use información contenida en un secreto industrial o comercial, sin consentimiento de la persona que lo guarda o de su usuario autorizado, con el propósito de obtener un beneficio económico para sí o para un tercero o de causar un perjuicio a la persona que lo guarda o al usuario autorizado será sancionado con prisión de cuatro a seis años."

Toda vez que la gran mayoría de las empresas guardan su información en servidores, unidades de almacenamiento, computadores y demás, estos se convierten en los objetos materiales de los delitos en cuestión. Por tal motivo se considera entonces bajo esta sección los **Delitos Financieros** y el **Espionaje Empresarial**.

> *"*243. Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita o haga uso indebido de dinero, 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 manipulación informática, fraudulenta o de medios tecnológicos**, será sancionado con prisión de cuatro a seis años."

> "288. Quien, para descubrir innovaciones o secretos de un agente económico, se **apodere de datos, información, soporte informático,** procedimiento, fórmula o informe, siempre que cause perjuicio a este, será sancionado con prisión de dos a cuatro años."

B. Otros delitos adecuados a la realidad tecnológica que no forman parte del Convenio de Budapest.

Cabe mencionar que existen otros delitos, que no necesariamente se encuentran bajo estos títulos o capítulos, pero que pueden ser cometidos mediante el uso de un equipo electrónico o informático, y que en efecto afectan la confianza en el uso de estos por los particulares como, por ejemplo:

- **Calumnia e Injuria**. (artículo 195) se cometa a través de un medio de comunicación social oral o escrito o utilizando un sistema informático.
- **Hurto**. (artículo 214 numeral 13) Cuando se cometa por medios tecnológicos o maniobras fraudulentas de carácter informático.
- **Daños a cosa mueble o Inmueble**. (artículo 230) Cuando el daño se ocasione utilizando instrumentos o medios informáticos, computadora, dato, red o programa de esa naturaleza.
- **Contrabando y Defraudación Aduanera**. (artículo 288-C numeral 4) Afecte el Sistema Informático Aduanero Oficial de la Autoridad Nacional de Aduanas al

introducir, alterar, modificar borrar, cambiar o anular declaraciones sin las debidas autorizaciones del administrador regional respectivo.

- **Terrorismo**. (artículo 295) utilice la Internet para enseñar a construir bombas o reclutar personas para realizar actos con fines terroristas.

3. Proyecto de Ley 632 de 2021

El panorama a futuro es ambiguo ya que, por un lado, tenemos un proyecto de Ley 632 de 2021 (Panamá, 2021) el cual propone varios cambios en la redacción y reestructuración de normativa penal y procesal penal los cuales consideramos no solo necesarios sino también positivos.

Ya en la exposición de motivos se establece claramente la intención y alcance, mismos que nos permitimos citar (parte de esta) de manera textual:

> "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 (botne/s), violación de los derechos de autor, pornografía infantil, pedo filia, 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."

Haciendo una revisión general sobre los cambios que se proponen con la citada Ley, podemos mencionar los siguientes:

- Incorporación de circunstancias agravantes generales en materia de tecnología ya por su uso o por ser el objeto material, en el Artículo 88 a saber:
    - "15. Cuando para la realización del hecho punible se utilice red de comunicaciones, cualquier medio de transferencia de datos, sistema informático, sistema electrónico, datos informáticos, comunicación electrónica, programas maliciosos o tecnología emergente.
      16. Cometer el hecho contra sistemas informáticos o sistemas electrónicos y similares pertenecientes a Infraestructura Crítica o Sistemas gubernamentales."
- Modificación a la redacción de la *Inviolabilidad del Secreto y el Derecho a la Intimidad*, así como la sanción que se establece en el artículo 166, la cual citamos y resaltamos en negrita los cambios introducidos:

- Quien posea legítimamente una correspondencia, **datos informáticos**, grabación o documentos privados y de carácter personal, no destinados **a hacerlo de conocimiento público**, aunque le hubieran sido dirigidos, y los haga públicos sin la debida autorización y de ello resultara un perjuicio, será sancionado **de dos a cuatro años de prisión**.
  No se considerará delito la divulgación de documentos indispensables para la comprensión de la historia nacional, las ciencias y las artes **o que constituyan pruebas de un delito denunciado ante el funcionario de investigación**.
  Si media el perdón expreso de la víctima, se ordenará el archivo de la causa,
  La sanción será de tres a cinco años si la conducta es realizada por un servidor público o persona particular, encargada o responsable de su custodia.

- Modificación algunos delitos relacionados a *Pornografía Infantil*, en cuanto a los artículos 184 y 185 se modifica tanto la redacción y la sanción (disminución), las que citamos y resaltamos en negrita los cambios introducidos:
  - "Artículo 184. Quien fabrique, elabore por cualquier medio o produzca material **de explotación sexual infantil** o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de un medio de **transferencia de datos, sistema informático, sistema electrónico, datos informáticos, comunicación electrónica, programas maliciosos o tecnología emergente o cualquier medio 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 **o personas con capacidades especiales**, si el autor pertenece a una organización criminal nacional o internacional o si el acto se realiza con ánimo de lucro."
  - "Artículo 185: Quien posea material pornográfico que contenga la imagen, real o simulada, de personas menores de edad, voluntariamente adquirido, será sancionado con pena de prisión de **tres a cinco** años.
    La pena será aumentada de una sexta parte a un tercio cuando se utilicen sistemas informáticos o medios de almacenamiento electrónico.*"*

- Así en la misma vía de los delitos relacionados a *Pornografía Infantil* se adiciona el artículo 184-A para salvaguardar la integridad de un menor o persona con discapacidad cuando se tenga conocimiento de evidencia (de delitos relacionados con pedofilia) se comunique con éste, aunque debemos resaltar que la redacción de este último artículo tiene oportunidad de mejora, a saber:
  - "Artículo 184-A: Quien, a sabiendas de existencia una evidencia previa y que éste, se comunique con un menor de edad o persona que posea discapacidad

que le impida expresarse voluntariamente, teniendo como finalidad la ejecución de un delito Contra la Libertad e Integridad Sexual, utilizando cualquier medio, inclusive un sistema informático, sistema electrónico o comunicación electrónica, 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."

- Adición del *ciberacoso (ciberbullying y cibergrooming)* en el artículo 204-A cuya redacción quedaría como:
    - "Artículo 204-A. Quien, a través de un sistema informático, sistema electrónico, comunicación electrónica, difunda, divulgue, reproduzca, retransmita o traspase datos informáticos, imágenes o videos, que afecten o atenten la integridad física, mental o emocional de una persona menor de edad, será sancionado con pena de seis a ocho 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, fonnación 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 capacidades especiales."
- Modificación a la redacción del artículo 226 sobre *Estafa y otros Fraudes* las cuales citamos y resaltamos en negrita los cambios introducidos, así como la incorporación de la *Suplantación de identidad* en el artículo 226-A:
    - "Artículo 226. Quien, para procurarse para sí o para un tercero un provecho ilícito, **ingrese**, altere, **borre**, **bloquee o desbloquee**, modifique o manipule **datos**, **o interfiera con el funcionamiento de un sistema informático o sistema electrónico**, en todo o en parte, 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 226-A. Quien suplante la identidad de una persona, para procurarse para sí o para un tercero un provecho ilícito, utilizando datos informáticos contenidos en un sistema informático, sistema electrónico, o tecnología emergente, será sancionado con pena de cuatro a seis años de prisión.

      Cuando la conducta cause un daño económico superior a los veinte mil balboas, la pena se aumentará a la mitad."
- Modificación a la redacción del artículo 243 sobre *Delitos Financieros* las cuales citamos y resaltamos en negrita los cambios introducidos:

- "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 **utilizando una red de comunicaciones, cualquier medio de transferencia de datos, sistema informático, sistema electrónico, datos informáticos, comunicación electrónica, programas maliciosos o tecnología emergente 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 proveedor de servicio**, empleado, trabajador, directivo, dignatario, administrador o representante legal de la entidad o empresa, aprovechándose de su posición o del error ajeno."

Sobre el Título VIII sobre Delitos contra la Seguridad Jurídica de los Medios Electrónicos, el cual reorganiza la redacción, clasificación distribución y esquematización de todo el Capítulo I de los Delitos contra la Seguridad Informática, mismos que por tema de espacio y dimensión del presente ensayo nos limitaremos a únicamente mencionar la distribución, esperando que el lector pueda hacer un estudio más detallado revisando el citado proyecto ley.

- **Artículo 289**. Sanciona el corte, ingreso, utilización o el permanecer conectado a un sistema informático o electrónico, o sus componentes. Adicionando una agravante de seis a ocho años cuando se trate de Infraestructura Crítica o gubernamental.
- **Artículo 289-A**. Sanciona el daño u obstaculización (total o parcialmente), o la afectación del funcionamiento de un sistema informático o electrónico, ya sea mediante bloqueo, alteración, deterioro, introducción, supresión de transmisión, borrado o supresión de datos informáticos. También adiciona agravantes cuando se trate de Infraestructura Crítica o gubernamental, o cuando sea realizado por lucro o beneficio propio o de un tercero.
- **Artículo 289-B**. Sanciona el llamado SPAM, o la emisión de mensajes electrónicos de forma masiva para engañar, confundir, causar daño, tomar controlo la destrucción de un sistema informático o electrónico.
- **Artículo 289-C**. Sanciona obtención y decodificación de códigos o sistemas de acceso para ingresar ilegítimamente a un equipo o sistema informático.
- **Artículo 290**. Sanciona la integridad de los datos estáticos (o que se encuentran almacenados).
- **Artículo 290-A**. Sanciona el apoderamiento o utilización de datos estáticos, aunque también adiciona agravantes cuando se trate de Infraestructura Crítica o gubernamental.

- **Artículo 290-B**. Sanciona la afectación a la transmisión de datos informáticos (en tránsito).
- **Artículo 290-C**. Sanciona la afectación a la seguridad o controles de acceso a sistemas informáticos.
- **Artículo 291.** Incorpora al catálogo de circunstancias agravantes a las *personas con capacidades especiales o población vulnerable o menores de edad* (en cuanto a la titularidad o propiedad de los sistemas informáticos, sistemas electrónicos, datos informáticos).
- **Artículo 292-A.** Sanciona la creación, uso, distribución (entre muchos verbos rectores que ofrece la reacción del artículo) de los llamados Virus, Malware y demás programas informáticos que tengan por objetivo afectar la integridad, seguridad o confidencialidad de los equipos informáticos o la información contenida en estos, siempre que se revelen públicamente, esto último de forma errada a nuestro criterio ya que condiciona el actuar del derecho penal a que el sujeto activo *haga público* los datos informáticos, claves, contraseñas o códigos de accesos.
- **Artículo 292-B.** Incorpora una agravante cuando se vulnere la confidencialidad de los datos obtenidos, o se afecte la intimidad o privacidad de las personas.

Por último, también se modifican artículos del Código Procesal Penal las cuales podrán ser objeto de un estudio posterior, pero que buscan mejorar el alcance y redacción de artículos en donde la materia tecnológica sea de importancia para el proceso penal.

4.Conclusiones

El proyecto de Ley 632 de 2021 (Panamá, 2021) propone varios cambios en la redacción y reestructuración de normativa penal y procesal penal los cuales consideramos no solo necesarios sino también positivos.

El llamado convenio de Budapest crea un abanico de figuras delictivas que sirven a los Estados para adecuar la legislación de los países, y de manera acertada, contempla los delitos informáticos bajo 4 títulos, que posteriormente pasaremos a estudiar de forma más amplia, a saber:

- Título 1 sobre Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- Título 2 sobre Delitos Informáticos
- Título 3 sobre Delitos relacionados con el contenido
- Título 4 sobre Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

En la actualidad, Panamá como signatario de dicho convenio, ha tenido que realizar adecuaciones a la normativa penal en esta materia, así tenemos que el Título VIII de Delitos contra la Seguridad Jurídica de los Medios Electrónicos, contiene un Capítulo I sobre Delitos contra la Seguridad Informática, donde establece 2 artículos (289 y 290) con figuras

delictivas que básicamente buscan incorporar todas las figuras que el convenio menciona en su llamado Título 1, y 2 artículos (291 y 292) con agravantes relacionadas a la materia o fuente de la información, o bien al sujeto que realiza la acción u omisión.

Sobre el Título VIII sobre Delitos contra la Seguridad Jurídica de los Medios Electrónicos, el cual reorganiza la redacción, clasificación distribución y esquematización de todo el Capítulo I de los Delitos contra la Seguridad Informática, mismos que por tema de espacio y dimensión del presente ensayo nos limitaremos a únicamente mencionar la distribución, esperando que el lector pueda hacer un estudio más detallado revisando el citado proyecto ley.

Por último, hacemos referencia al proyecto de Ley 632 de 2021 el cual propone cambios y reestructuración, desde nuestro punto de vista adecuados y necesarios, de cara a fomentar en el lector un carácter crítico de promotor de este proyecto ley el cual estamos completamente seguros de que traerá muchos beneficios a nuestra legislación penal en materia de ciberdelincuencia.

5.Bibliografía

Arango Durling, V. (2009). *Delitos contra el sistema o por medios informáticos.* Panamá: Anuario de Derecho.

Arboleda Vallejo, M., & Ruiz Salazar, J. A. (2001). *Manual de Derecho Penal - Parte Especial.* Leyer.

Muñoz Pope, C. E. (2003). *Introducción al Derecho Penal.* Panamá: Ediciones Panamá Viejo.

Muñoz Pope, C. E. (2003). *Introducción al Derecho Penal.* Panamá: Ediciones Panamá Viejo.

Ossorio, M. (1999). *Diccionario de Ciencias Jurídicas Políticas y Sociales - 1ª Edición Electrónica.* Guatemala, C.A.: Realizada por Datascan, S.A.

Ossorio, M. (s.f.). *Diccionario De Ciencias Juridicas Politicas y Sociales.* Datascan, S.A.

Panamá, A. N. (12 de Octubre de 2021). *Proyecto de Ley 632 de 2021*. Obtenido de https://www.asamblea.gob.pa/APPS/SEG_LEGIS/PDF_SEG/PDF_SEG_2020/PDF_SEG_2021/2021_P_632.pdf

RAE. (Octubre de 2014). *Real Academia de la Lengua Española*. Obtenido de Real Academia de la Lengua Española: http://lema.rae.es/drae/?val=informacion

KURT BEERMANN HERMMERLING

Licenciado en Derecho y Ciencia Política de la Universidad de Panamá.
Maestría en Derecho con énfasis en Derecho Penal. Universidad de Panamá.
Maestría en Docencia Superior, Universidad Latina.
Profesor de Derecho Penal, Universidad de Panamá, 2023.

Artículo recibido: 16 de octubre de 2023
Aprobado: 20 de noviembre de 2023