ESTUDIO DE RECOMENDACIONES SOBRE CIBERDELINCUENCIA

La "*Evolución Tecnológica*" , ha transformado el mundo y la forma en que las personas realizamos las diferentes actividades sean cotidianas, económicas, académicas, de servicios, comunicación, producción, entre otros.

Dicha evolución, también ha incidido en la forma en que se realizan las actividades delictivas, donde la tecnología es utilizada como "*medio*" para cometer delitos comunes y de crimen organizado, o bien, como "*objeto*" de la actividad delictiva.

El delito informático ha sido definido como aquella "*acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas -hardware- o de los programas –software"*[1]

Los delitos informáticos tiene como características que: a) son de rápida ejecución y alto alcance, b) de fácil encubrimiento, c) novedosos, d) no siempre son fáciles de tipificar, e) generan nuevos bienes jurídicos tutelados, f) son intangibles, g) difíciles de vigilar, h) transitorios por su naturaleza, i) pueden ser disociados en el tiempo, j) difícil identificación del autor, por lo tanto, son difíciles de investigar, perseguir y juzgar.

La ciberdelincuencia, es una amenaza que si bien es cierto actúa de forma silenciosa, el daño es de gran impacto, generando pérdidas a nivel mundial, siendo que, durante el año 2016, de acuerdo con estudios realizados, se estima que el total de costos financieros causados por la ciberdelincuencia durante dicho año, supera los US$125.900 millones de dólares.[2]

[1] Chinchilla Sandí, Carlos. (2004) Delitos Informáticos: Elementos básicos para identificarlos y su aplicación. San José, Costa Rica. Ediciones Farben

[2] Informe Norton Ciberseguridad 2016 recuperado el 30-May-2017 en https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf

Las tendencias futuras en el incremento del cibercrimen, están orientadas a actividades como : el "*Crime-as-a-Service*", "*Ransomware*", "*Uso criminal de datos*", "*Fraude de pago*", "*Abuso sexual infantil en línea*", "*Abuso de la Darkenet*", "*Ingeniería Social"*, "*Monedas Virtuales*"[3], así como el ataque a infraestructuras críticas, lo cual pone en peligro vidas humanas y la economía de los países.

Estudios han señalado que los marcos jurídicos relacionados con la ciberseguridad y la ciberdelincuencia, de los diversos países de la región se encuentran aún en una etapa incipiente, en cuanto a la promulgación de leyes relacionadas con la materia.

A continuación, se presenta un cuadro referente a la situación de cada país, cuyos datos fueron extraídos del informe denominado *"Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Informe Ciberseguridad 2016",* realizado por el Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID).

Dicho estudio realiza una evaluación, donde identificaron cinco niveles de madurez de la capacidad de seguridad cibernética en Latinoamérica, a saber: "*Inicial*", "*Formativo*", "*Establecido*", "*Estratégico*" y "*Dinámico*". Para efectos del cuadro, se representarán con los valores: 1, 2, 3, 4 y 5, respetivamente.

Si bien es cierto, el estudio realizado por la OEA, no hace relación al sistema jurisdiccional propiamente dicho, el mismo sirve de base, para tener una visión global de la situación actual de algunos de los países miembros, puesto que, no se abarca a los países ibéricos.

[3] http://www.ituser.es/seguridad/2016/10/europol-presenta-su-informe-sobre-el-cibercrimen-en-europa

Ahora bien, en relación con el "***Derecho Penal Sustantivo***", cada uno de los niveles se valora de la siguiente manera:

1: "*El derecho penal sustantivo específico para la delincuencia cibernética no existe, o existe el derecho penal general y se aplica ad hoc a la delincuencia cibernética".*

2: *"Existe una legislación parcial en el derecho penal sustantivo que aplica losmarcos legales y regulatorios a algunos aspectos de los delitos cibernéticos; está siendo discutido el derecho penal sustantivo para la delincuencia cibernética entre los legisladores, pero ha comenzado el desarrollo de la ley".*

3: *"La legislación vigente tipifica una serie de delitos relacionados con pruebas electrónicas que pueden ser objeto de una legislación específica o abordados en el código penal".*

4: *"El país se adhiere a las mejores prácticas y normativas regionales e internacionales pertinentes sobre derecho de delito cibernético y asigna los recursos de acuerdo a las prioridades nacionales".*

5: *"El país continuamente busca incluir el desarrollo de las mejores prácticas internacionales sobre delito cibernético en la legislación nacional y es un colaborador activo en el discurso global sobre la mejora de los instrumentos de la lucha contra delitos cibernéticos internacionales; existen medidas para superar en el país las líneas de base mínimas de seguridad internacional".*

En cuanto al "***Derecho procesal de delincuencia cibernética***", los niveles valoran lo siguiente:

1: *"No existe el derecho penal procesal adecuado para la delincuencia cibernética*

y el uso de la prueba electrónica en otros crímenes, o existe el derecho penal procesal general y se aplica ad hoc a la delincuencia cibernética y al uso de la prueba electrónica en otros crímenes".

2: *"Se está discutiendo y desarrollando el derecho procesal penal en relación con la prueba electrónica; el derecho procesal penal se aplica ad hoc a la delincuencia cibernética, pero no ha comenzado el desarrollo de los delitos cibernéticos específicos".*

3: *"Se ha implementado el derecho procesal penal integral y los requisitos probatorios relacionados; las mejores prácticas se emplean por aplicación de la ley en el ejercicio de poderes procesales".*

4: *"En el caso de la investigación transfronteriza, el derecho procesal estipula las acciones que es necesario realizar bajo las características de casos particulares, con el fin de obtener con éxito la prueba electrónica".*

5: *"El país se adhiere a las mejores prácticas internacionales sobre procedimiento penal de delito cibernético y la obtención de pruebas electrónicas, y constantemente busca implementar estas medidas en la legislación nacional y sirve como un colaborador activo en el discurso global sobre la mejora de la lucha contra los delitos cibernéticos internacionales; existen medidas para superar las líneas de base mínimas de seguridad internacional, que contribuyen al desarrollo de mejores prácticas internacionales".*

Y en lo que se refiere al "***Cumplimiento de la ley***", el estudio señala que:

1: *"No existe la capacidad de las autoridades policiales para prevenir y combatir los delitos relacionados con la cibernética".*

2: *"Existe alguna capacidad de investigación para indagar delitos que involucren pruebas electrónicas, así como para obtener dichas pruebas, de conformidad con el derecho interno; sin embargo, esta capacidad es mínima".*

3: *"Se ha establecido una capacidad institucional integral para investigar y manejar casos de delincuencia cibernética y delitos relacionados con pruebas electrónicas, incluyendo los recursos humanos, procesales y tecnológicos, medidas exhaustivas de investigación, cadena de custodia digital y gestión de integridad de las pruebas y mecanismos formales e informales de colaboración con interesados internacionales y nacionales (actores de los sectores privado y público)".*

4: *"Los oficiales de las fuerzas de la ley reciben una formación continua basada en las responsabilidades relativas y en entornos de amenazas nuevas y cambiantes y pueden utilizar herramientas forenses digitales sofisticadas para investigar delitos informáticos complejos y delitos relacionados con pruebas electrónicas; los organismos locales de aplicación de la ley colaboran con contrapartes regionales e internacionales en investigaciones".*

5: *"Existen recursos dedicados a unidades de delitos informáticos plenamente operativas, incluyendo capacidades avanzadas de investigación y de gestión de integridad de los datos; es posible recoger y analizar las estadísticas y tendencias que mejorarían la investigación sobre los delincuentes con el fin de facilitar una comprensión exhaustiva del ambiente delictivo en línea y contribuir a la toma de decisiones estratégicas; las agencias de aplicación de la ley nacionales están participando plenamente en la investigación y redes transfronterizas".*

País	Derecho sustantivo de delincuencia cibernética	Derecho procesal de delincuencia cibernética	Cumplimiento de la ley
Argentina	3	3	3
Bolivia	2	2	2
Brasil	3	4	4
Chile	3	4	3
Colombia	3	3	3
Costa Rica	3	3	3
Ecuador	3	2	2
El Salvador	2	2	2
Guatemala	2	1	2
Honduras	2	1	1
México	3	2	4
Nicaragua	1	3	1
Panamá	3	2	2
Paraguay	3	2	2
Perú	3	2	2
República Dominicana	5	5	5
Uruguay	1	2	2
Venezuela	3	1	2

Para conocer cuál es la situación real de cada país, en relación con su legislación referente a los delitos informáticos, se considera oportuno realizar un estudio a través de una matriz, donde se especificarán los tipos penales, leyes especiales o procesales de sus legislaciones, así como la estructura organizativa, jurisprudencia y convenios suscritos por sus respectivos estados.

A partir de este estudio de campo, se podrá precisar el estado en que se encuentra cada país, en relación a este tipo de hechos punibles, y a partir de allí dictar recomendaciones, o bien, este podrá ser de utilidad para cada uno a efecto de que tomen las precauciones y realicen las iniciativas que consideren oportunas, para armonizar sus legislaciones conforme a los nuevos estándares internacionales.

Un aspecto importante a considerar, es que en la medida que los países tengan armonizada la normativa jurídica, con el resto de la región, la misma, facilitará mayor cooperación internacional, con el fin de perseguir y castigar a los partícipes de este tipo de hechos, y consecuentemente facilitar la extradición tanto activa, como pasiva, de este tipo de conductas al margen de la ley.

Es por lo anterior que se recomienda a los países miembros de la Cumbre Judicial Iberoamericana, promover los mecanismos jurídicos, procesales y de cooperación internacional, que faciliten la lucha contra este tipo de criminalidad, razón por la cual, se presenta el siguiente informe, el cual muestra un catálogo de tipos penales, utilizados en los diferentes países para sancionar conductas delictivas relacionadas con el ciber-crimen.

ESTUDIO NORMATIVO RELACIONADO CON EL CIBERCRIMEN

Se solicita a cada uno de los países de Cumbre Judicial, llenar el siguiente formulario, el cual nos permitirá obtener los insumos necesarios, para precisar las normas que regulan los delitos determinantes o que se refieran al ciber-crimen, así como, jurisprudencia relacionada y la estructura organizacional de las instituciones involucradas en este tipo de actividades ilícitas.

El documento se ha dividido en cuatro puntos:

I. Legislación de los países miembros de la Cumbre Judicial Iberoamericana, relacionada con los delitos informáticos
II. Convenios Internacionales ratificados y/o en trámites de ratificación en los países miembros.
III. Jurisprudencia relacionada con ciberdelincuencia en los países miembros.
IV. Estructura organizativa en el marco de los delitos informáticos, donde se incluya la Policía Judicial, Ministerio Público y la Judicatura

FORMULARIO
ESTADO ACTUAL DE LA CIBERDELINCUENCIA EN LOS PAÍSES DE CUMBRE JUDICIAL IBEROAMERICANA

País: _____

Nombre contacto del país: _____

Correo electrónico: _____

El presente formulario tiene como objetivo elaborar un mapeo sobre el estado de las legislaciones de los países en relación con la Ciberdelincuencia.

I. LEGISLACIÓN DE LOS PAÍSES MIEMBROS DE LA CUMBRE JUDICIAL IBEROAMERICANA, RELACIONADA CON LOS DELITOS INFORMÁTICOS

Este apartado se ha divido en dos áreas: normas sustantivas y normas procesales. Para complementar los datos, la tabla se divide en cinco columnas, a saber:

a) **Tipo penal de referencia:** En esta columna se presentan algunos tipos penales que se encuentran incorporados en el derecho positivo. El dato allí señalado, debe considerarse sólo como referencia, por cuanto, el "*nom iuris*" en cada país podría variar.
b) **Artículo:** Se debe anotar el número del artículo
c) **Cuerpo normativo:** Nombre del cuerpo normativo donde se encuentra tipificada la norma
d) **Nombre de la norma:** "*Nom iuris*" conforme a la legislación del país estudiado
e) **Descripción del tipo penal:** Descripción literal del tipo penal

Además, es importante destacar que los tipos penales de referencia aquí anotados, son una guía, no obstante, cada país puede incorporar aquellos que tengan en su legislación y que no se encuentren aquí señalados.

- **Normas jurídicas sustantivas relacionadas con ciberdelincuencia**

Tipo Penal de referencia	Artículo	Norma	Nombre de la norma (conforme a su legislación)	Texto de la norma
DELITO INFORMÁTICO COMO MEDIO DE LA ACCIÓN DELICTIVA				
Delitos Sexuales				
Corrupción				
Seducción o encuentros con menores por medios electrónicos (Grooming)				
Turismo sexual				
Fabricación, producción o reproducción de pornografía				
Pornografía virtual y pseudo pornografía				
Tenencia de material pornográfico				
Difusión de pornografía				
Delitos contra el ámbito de intimidad				
Violación de correspondencia o comunicaciones				
Violación de datos personales.				

Delitos contra la propiedad				
Extorsión informática (Ransomware)				
Estafa informática				
Daño agravado				
Narcotráfico y crimen organizado				
Espionaje				
DELITO INFORMÁTICO COMO OBJETO DE LA ACCIÓN DELICTIVA				
Delitos informáticos y conexos				
Sabotaje informático				
Daño informático				
Suplantación de identidad				
Espionaje informático				
Instalación o propagación de programas informáticos maliciosos				
Suplantación de páginas electrónicas				
Facilitación del delito informático				
Difusión de información falsa				

- **Normas jurídicas procesales relacionadas con ciberdelincuencia**

Norma procesal de referencia	Artículo	Cuerpo normativo	Nombre de la norma (conforme a su legislación)	Descripción de la norma procesal penal

II. CONVENIOS INTERNACIONALES RATIFICADOS Y/O EN TRÁMITES DE RATIFICACIÓN

Indicar aquellos convenios internacionales ratificados, o en proceso de ratificación, en su país.

a) **Nombre convenio:** Señalar el nombre del convenio
b) **Estado:** Se refiere si el mismo está ratificado, o bien, se encuentra en pendiente o en proceso de ratificación
c) **Fecha de promulgación:** En caso de estar ratificado, indicar la fecha de promulgación
d) **Fecha de ratificación:** Señalar la fecha de ratificación en su país

Nombre Convenio	Estado	Fecha de promulgación	Fecha de ratificación

III. JURISPRUDENCIA RELACIONADA CON CIBERDELINCUENCIA

Con el fin de obtener información de criterios jurisprudenciales de los diversos países, se considera oportuno, obtener las resoluciones emitidas por los altos tribunales (Tribunales o Sala de Casación), relacionados con los delitos informáticos

a) **Tribunales de Apelación o Sala de Casación:** Indicar el nombre órgano que dicta la resolución
b) **No. Voto o Sentencia:** Anotar el número de voto o sentencia, que la identifique
c) **Fecha:** Fecha de emisión del voto o sentencia
d) **Tipo Penal:** Indicar el tipo penal que fue objeto de discusión en el recurso
e) **Nombre documento adjunto:** Indicar el nombre del documento que se adjunta a este formulario con el contenido del voto o sentencia señalado.

Tribunal de Apelación o Sala de Casación	No. Voto	Fecha	Tipo penal	Nombre documento adjunto

IV. ESTRUCTURA ORGANIZATIVA EN EL MARCO DE LOS DELITOS INFORMÁTICOS

Con el fin de conocer la estructura organizativa de cada Institución, relacionada con los delitos informáticos, se considera oportuno conocer, si en los países miembros, se cuenta con unidades de especialización creadas para investigar, combatir y judicializar, los hechos punibles cometidos a través del uso de la tecnología informática, desde la investigación, recolección, manejo de evidencia y prueba digital, entre otros. Por ejemplo, si existen Fiscalías, Unidades de la Policía o Jurisdicciones especializadas en Delitos Informáticos.

En caso de no existir unidades especializadas, indicar cuál es la estructura utilizada.

a) **Institución:** Nombre de la oficina
b) **Funciones:** Indicar las funciones que realiza dicha unidad

Institución	Funciones
Policía Judicial	
Ministerio Público	
Judicatura	