UNIVERSIDAD HISPANOAMERICANA

FACULTAD DE DERECHO

TESIS PARA OPTAR EL GRADO DE LICENCIATURA EN DERECHO

ANÁLISIS JURÍDICO SOBRE LA CIBERDELINCUENCIA Y SUS POSIBLES REFORMAS A LA LEGISLACIÓN COSTARRICENSE.

Sustentante:
Jean Carlo De la Sera Muñoz

Tutor:
Francisco Fonseca Ramos

Setiembre 2018

II CUATRIMESTRE, 2018

APROBADO: _____

PENDIENTE: _____

CONTENIDO

DEDICATORIA…… ……...III
AGRADECIMIENTO……..IV

CAPITULO I: PROBLEMA DE INVESTIGACIÓN……..7
1.1. PLANTEAMIENTO DEL PROBLEMA……...8
1.1.1. Antecedente del problema……..10
1.1.2. Problematización 13
1.1.3. Justificación del Tema 15
1.2. FORMULACIÓN DEL PROBLEMA 18
1.3. OBJETIVOS DE LA INVESTIGACIÓN 19
1.3.1. Concepto de Objetivo General 20
1.3.2. Objetivo General de la investigación 21
1.3.3. Objetivos específicos 22
1.3.4. Objetivos específicos de la investigación 23
1.4. ALCANCES Y LIMITACIONES 24
1.4.1. Alcances 25
1.4.2. Limitaciones 25
CAPITULO II: MARCO TEÓRICO……..26
2.1. CONTEXTO HISTÓRICO 27
2.1.1. Raices de la cibercriminalidad 27
2.1.2. Lucha contra la ciberdelincuencia a nivel del Consejo de Europa…..32
2.1.3. Costa Rica como pais vanguardia a la luz del acontecer historico a nivel del derecho penal informatico nacional……36

2.2. CONTEXTO TEORICO……..…….64
2.2.1. Conceptualización del delito informático……..……..……64
2.2.2. Ciberdelitos y su derecho comparado en Latinoamerica y España…….……..…69

2.2.2.1 México……..……..69

2.2.2.2 Guatemala……..……..……..……...77

2.2.2.3 Panamá…….……..…81

2.2.2.4 Colombia……..……....86

2.2.2.5 Argentina……..……..94

2.2.2.6 España…….……100

2.2.3 El Convenio de Budapest a la luz de la Legislación Sustantiva Costarricense……...…108

2.2.3.1 El Hacking y sus formas de ensayo a nivel Internacional……..……126

2.2.4 Judicialización de los ciberdelitos y la obtención de la prueba en el exterior……..130

2.2.4.1 El Cibercrimen como conocimiento y su aplicación práctica……..130

2.2.4.2 La Evidencia Digital……..……136

2.2.4.3 Fundamento Jurídico Nacional para la obtención de la prueba en el exterior…….....149

2.2.4.4 Fundamento Jurídico para la obtención de la prueba a nivel consular.152

2.2.4.5 Fundamento Jurídico para la obtención de la prueba por la Autoridad Central……..…152

2.2.4.6 Convención de Nassau…….…153

2.2.4.7 Convención de las Naciones Unidas contra la Delincuencia Organizada (Convención de Palermo)……..154

2.2.4.8 Oficina de Asesoría Técnica y Relaciones Internacionales ……..…..156

2.2.4.9 Asistencia Jurídica Internacional…….…158

2.2.4.10 Procedimiento Consular para la obtención de la prueba digital……160

2.2.4.11 Procedimiento por Autoridad Central para la obtención de prueba digital……..…161

2.2.4.12 La Prueba Espuria…….163

2.2.4.13 El papel de la Sección de Delitos Informáticos……..…166

2.2.4.14 Proyecto de Ley N° 21187……169

2.3. HIPÓTESIS 171

2.3.1. Concepto 171

2.3.2. Hipótesis de la Investigación 172
2.3.3. Variable independiente 173
2.3.4. Variable independiente de la investigación 174
2.3.5. Variable dependiente 175
2.3.6. Variable dependiente de la investigación 176
2.4. OPERACIONALIZACIÓN DE LA HIPÓTESIS 177
CAPITULO III: MARCO METODOLÓGICO……..….....179
3.1. TIPO DE INVESTIGACIÓN 180
3.1.1. Finalidad 181
3.1.2. Dimensión temporal 182
3.1.3. Marco 183
3.1.4. Naturaleza 184
3.1.5. Carácter 186
3.2. SUJETOS Y FUENTES DE INVESTIGACIÓN 187
3.2.1. Fuentes de primera mano 188
3.3. SELECCIÓN DEL MUESTREO 190
3.3.1. La población 191
3.3.2. La muestra 190
3.3.3. No probabilística 192
3.4. TÉCNICAS E INSTRUMENTOS PARA DESARROLLAR LA INVESTIGACIÓN 193
3.4.1. La investigación documental 195
3.4.2. Estudio de caso 196
3.5. DEFINICIÓN CONCEPTUAL, OPERATIVA E INSTRUMENTAL DE LAS VARIABLES 197
3.5.1. Definición conceptual 197
3.5.2. Dimensión 198
3.5.3. Definición conceptual de la dimensión 199
3.5.4. Definición operacional 200
3.5.5. Definición Instrumental 201
3.5.6 Cuadro de operacionalización de las variables: 202
4. ANALISIS E INTERPRETACION DE DATOS……203
4.1 Entrevista a Licenciada Sharon Segura……..……..…203

4.2 Entrevista a Freddy Bautista……205

4.3 Entrevista al Licenciado José Adalid Medrano……208

5.CONCLUSIONES Y RECOMENDACIONES……212

5.1 CONCLUSIONES……212

5.2 RECOMENDACIONES……213

BIBLIOGRAFIA……214

GLOSARIO……232

ANEXOS……233

ANEXO 1 Cuadro 1……234

ANEXO 2 Mapa Conceptual……236

ANEXO 3 Matriz de Gestion……237

ANEXO 4 Cuadro 2……238

ANEXO 5 Borrador del Instrumento……239

ANEXO 6 Hoja de Aprobacion del Tema……240

ANEXO 7 Rubrica de Seminario……241

DEDICATORIA

Me encuentro con muchos sentimientos encontrados al redactar esta página, y eso se refiere a la gran lucha que tuve para llegar donde estoy hoy. En primer lugar, quiero dedicar este trabajo de investigacion a mi madre Adriana Muñoz Gómez, por toda la crianza que me dio siendo un niño, como adolescente y ahora en esta etapa se merece todo, por ella soy lo que soy. Luego, a mi padre Carlos De la Sera, por ser un trabajador incansable para proveer alimentos al hogar desde toda la vida, gracias por enseñarme a ser un guerrero y a mi hermano Alexander De la Sera, que es como un gemelo, una parte de mi cuerpo, le dedico este trabajo con mucho afecto y amor.

Se lo dedico también a mi abuela Virginia Gómez, a quien quiero mucho y ojalá Dios le muchos años más de vida, para que vea el cumplimiento de mis próximas metas como profesional, y más títulos. A mi tía Karla Muñoz, se lo dedico con sumo cariño puesto que fue la que me ayudo a matricular el primer cuatrimestre, sin tener trabajo, nunca me olvido de ese día, esto se da gracias a usted, y a mi tío Víctor Muñoz, le dedico este trabajo con mucho cariño, ya que fue un puente para cumplir mis metas y mis sueños, es él un reflejo de que lo que el trabajo, la pasión y milla extra puede dar en un futuro, esto se debe a usted también.

Y, por último, esta dedicatoria va dirigida a Nicole De la Sera, Aharon Arias y Fabiola Arias, que es la próxima generación en la familia, si yo pude ustedes también, estudien bastante, para que sean profesionales. Los amos a todos.

AGRADECIMIENTO

Agradezco infinitamente al señor todopoderoso que nos da un día más de vida, por el más grande estoy aquí escribiendo y cumpliendo mi sueño. Luego agradezco a todos los compañeros de universidad, excompañeros de los diferentes trabajos que he laborado, y amigos que lo ayudan en este camino. Le agradezco especialmente a Michelle Solano, por toda la colaboración que me brindó durante esta travesía y a la Licenciada Carolina Rodríguez, que solo les puedo decir gracias.

Agradezco a la Licenciada Marta Cedeño Jiménez y a la señora Gloria Portilla por darme la oportunidad de laborar en la oficina, mientras me encontraba realizando la tesis, ya que me tratan como un hijo, lo único que me queda decir es gracias a todos.

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1. PLANTEAMIENTO DEL PROBLEMA

La presente investigación tiene estricta relación con los fenómenos delictivos que acompañan las nuevas tecnologías, cada vez es mucho más común que los ciberdelitos se encuentren presentes en el quehacer diario, pues como ciudadanía globalizada, se vive en un mundo dependiente de la tecnología.

El hecho de que una persona tenga en sus manos un dispositivo móvil lo hace ser participe del ciberespacio, pues, se debe entender que es un espacio no físico, donde cientos de cibernautas se encuentran navegando en la red de Internet, en razón de ello, se puede ser víctimas de un ciberdelito, pues para serlo únicamente se ocupa estar conectado en la ciber red.

Al indicar que se está frente una nueva era de criminalidad, brinda nuevas herramientas a los delincuentes informáticos para realizar sus fechorías, pues la tecnología todos los días avanza en pasos gigantescos, y por esa razón las legislaciones siempre van a estar un paso atrás de las fechorías de los hackers, pues ellos poseen un conocimiento más especializado en el área del cibercrimen, que los propios juristas, legisladores.

La globalización de hoy, exige que tanto los operadores del derecho, administradores de justicia, legisladores, se encuentren totalmente empapados del fenómeno del cibercrimen, pues es una realidad que se debe combatir con todas

las fuerzas, y para ello se exige una legislación, la cual pueda atender de una manera eficiente los ciberdelitos, por ello se determinara en este proceso de investigación si Costa Rica es suficientemente capaz de tutelar el fenómeno cibernético, de una manera adecuada la ciberdelincuencia en todos sus aspectos.

Es un hecho notorio de las nuevas tecnologías (TICS) que permiten comunicarse con cualquier persona, en cualquier lugar del mundo, así de poderosa es el Internet, dado esta característica es transnacional, el cibercrimen no posee fronteras ni barreras, por ende, los ciberdelincuentes aprovechan la facilidad que da el Internet para cometer las fechorías informáticas, en cualquier lugar y hace muy complejo el rastreo de donde se cometió el delito, pues no siempre la dirección IP del servidor va ser en realidad la correcta. Pueden utilizar artificios tecnológicos para ocultar su dirección IP como VPN o inclusive los Servidores Proxy, por ende, su ubicación no siempre va a ser rastreable.

Además, por la transnacionalidad de este fenómeno, la evidencia digital en la mayoría de los casos que se investigan la prueba se encuentra en el exterior, fuera del país y ello resulta fundamental para determinar la autoría o no del ciberdelito, pues con ello como en un Estado de Derecho el juez tendría la total certeza de la culpabilidad o no del sujeto. Por ende, las nuevas herramientas tecnológicas permiten un sinfín de situaciones que favorecen al ciberdelincuente, por esa razón, lo hace aún más difícil.

1.1.1. Antecedente del problema

El inicio de la cibercriminalidad informática, va de la mano con la aparición del Internet en donde el primer fenómeno delictivo que se derivó de las nuevas tecnologías fueron los malware o virus maliciosos en las computadoras, en el año 1995 con la creación de Microsoft Windows 95, surgieron nuevos virus, los cuales tenían como meta dañar los documentos de Word conocidos como Concept y que en realidad la propagación de virus o malware llegó a ser el más conocido en ese tiempo. Posteriormente en el año 1996 un grupo de informáticos crea el virus Australia Boza O Bizatch, este infectaba archivos de 32 bits a través del programa Microsoft Windows Nt. (Laboratorio Eset de Latinoamérica, 2012)

La inserción de un malware en un computador fue la primera conducta ilícita referente a la delincuencia informática, se dio en los años noventa, es un ilícito antiguo, y ha acompañado al nacimiento de otros delitos informáticos, que tienen sus repercusiones hoy. Inclusive, existe una teoría de otros estudiosos, ellos indican que quienes crearon los malware, la infección de los virus en los computadores, son los creadores actuales de los Antivirus utilizados actualmente en las máquinas.

En vista de todos los hechos delictivos que se daban en ese momento como el daño cibernético a la gran empresa Microsoft en su condición de víctima, el Consejo de Europa dentro de sus facultades decidió formar un Comité de

Especialistas que se dedicaran al estudio de las nuevas tecnologías (TICS), el fenómeno de la delincuencia informática, donde tenían como misión luchar en contra la ciberdelincuencia.

Dadas las complejidades que afronta el cibercrimen, surgieron diferentes foros, donde diversas entidades como Organización de Estados Americanos (OEA), se vieron involucrados y allí Costa Rica propuso la creación de un Convenio Interamericano sobre Delitos Informáticos, por las ventajas que hubiesen conllevado un marco de leyes-tipo. A inicios del año 2004 se dio una ventana de opiniones del cual se denominó Foro Legislativo en Materia de cibernéticos, organizado por la Organización de Estados Americanos, en este se discutió nuevamente la elaboración de la normativa latinoamericana, y se arribó a la conclusión que no existía ningún avance, ni tampoco un apoyo político fuerte para su respectiva firma por los Estados Americanos, inclusive Estados Unidos de América rechazó formar parte del mismo, pues ya había firmado el Convenio de Budapest, y consideraban que era innecesario, pues ya existía un Tratado Internacional.

Por parte del Consejo de Europa invitó a Costa Rica desde el 2004 a formar parte del Convenio de Budapest, donde el fin era agregarse en el mismo, y tener una política penal común entre los países firmantes, ya que al ser la ciberdelincuencia transfronteriza debían contar con una cooperación internacional, la cual pudiese luchar en contra del cibercrimen.

Debido a la trascendencia del Internet, en el mundo entero, conlleva a facilidades que el ciberdelincuente aprovecha, como la imposibilidad de rastrear la ubicación del sujeto, si cuenta con un servidor proxy, o si más bien navega en la Deep web y gestiona los delitos cancelando una suma módica en Bitcoin, Monero, diversos artificios que hacen compleja la investigación y por esa razón los Estados ocupan de cooperación internacional.

El ciberdelincuente tiene a disposición una serie de herramientas tecnológicas para encubrir sus fechorías en el ciberespacio, por esa razón este proyecto de investigación se basará en que si Costa Rica cuenta con la capacidad de tutelar la ciberdelincuencia como también si puede recolectar evidencia digital del extranjero que venga a facilitar la investigación del proceso penal.

1.1.2. Problematización

Las nuevas tecnologías convierten al fenómeno de la ciberdelincuencia en complejas, pues debe considerarse que los delincuentes informáticos pueden estar realizando el delito en otro país, o inclusive manejan una dirección IP falsa, por esa razón, se convierte en anónimo el cibercrimen y que debe ser abordado por un trabajo en conjunto con los demás países, es una lucha transnacional. La Asamblea Legislativa (2012) expresa que:

> Cabe indicar que, precisamente por la extensa cantidad de redes de cómputo dentro y fuera de los países, así como la incursión de la Internet, nos enfrentamos a un serio problema de territorialidad que solo puede verse solventado con la aplicación de acuerdos internacionales y la adopción de medidas técnicas uniformes en los diferentes territorios donde se pretenda perseguir penalmente a los infractores cibernéticos. (p.8)

Por la globalización actual, la cual no conoce fronteras, la gran parte de la información requerida para realizar la investigación, siempre se encuentra en el extranjero, es decir, todas las empresas están domiciliadas normalmente en Estados Unidos, por esa razón la evidencia digital siempre se requerirá de la ayuda de otros Estados para la obtención de la prueba que se agregará al proceso penal correspondiente.

.

Considerando el cibercrimen, como una problemática de la actualidad y que avanza todos los días, es decir, cada día que pasa el ciberdelincuente se vuelve más astuto, tiene más conocimiento, lo cual conlleva al aumento de los casos de delitos informáticos. Es un conocimiento especializado que poseen y por esa razón siempre buscarán los medios tecnológicos de delinquir de diversas formas, no siempre va ser la misma conducta, sino que se apoyarán en las herramientas brindadas por la tecnología para realizar las fechorías de una forma novedosa, y que complique la labor policial.

Por las nuevas formas que tiene el ciberdelincuente de delinquir en el ciberespacio, es necesario que Costa Rica, cuente con un marco jurídico que pueda atender todas las causas penales referentes a los delitos informáticos.

También, se debe observar que la evidencia digital al ser tecnológica permite que la misma pueda ser borrada y no dejar ningún rastro sobre el delito informático cometido, por eso el tiempo de respuesta de los diferentes países para la obtención de la prueba, es crucial para definir o no la autoría del ciberdelincuente. Todas estas variables, deberán ser determinadas si el Estado Costarricense, es capaz de dar una tutela efectiva del delito informático en todos sus ámbitos.

1.1.3. Justificación del Tema

Este trabajo de investigación se fundamenta al alcance que tiene el Internet, actualmente los seres humanos dependen tecnológicamente de un dispositivo móvil, un computador, para poder desarrollarse en cualquier ámbito sea profesional, laboral, es decir, todos los días los ciudadanos están inmersos en la tecnología que permite ser un blanco fácil para los ciberdelincuentes.

Por el auge que han tenido las nuevas tecnologías en el entorno, se hace imperativo incorporarse al ciberespacio, este es un espacio no físico donde miles de personas navegan en la red de internet o en la Deep web, con el simple hecho de encontrarse conectados al ciberespacio, se puede ser víctima de un ciberdelito.

La gran mayoría de veces, los cibernautas desconocen si realmente fueron víctimas de un delito informático, pues la ciberdelincuencia es un hecho silencioso, el cual afecta enormemente a las personas y a las empresas. En el caso de las empresas que son víctimas del cibercrimen en demasía, nunca les comentan a sus clientes que fueron hackeados, pues, está en juego su reputación, la fama dentro del mercado, luego entran aspectos de competencia con otra marca o empresa, entonces es una tendencia actual, la cual afecta a millones de sujetos, y también el cibercrimen es muy rentable.

Esta tendencia del cibercrimen viene a marcar un paradigma en las nuevas investigaciones policiales, pues, deben de estar lo suficiente actualizado para luchar eficazmente en contra de la ciberdelincuencia, ya que la tecnología avanza todos los días y los delincuentes están buscando la manera de mejorar sus técnicas delictivas, para complicar aún más la investigación.

Es un reto para las autoridades policiales luchar contra el cibercrimen, pues, es un fenómeno que no solamente lo realizan hackers aislados, sino que más bien ya existen grupos criminales ubicados en los distintos países para llevar a cabo las fechorías tecnológicas. Con solamente que exista una unión de delincuentes informáticos, ya se está hablando de crimen organizado, antes se pensaba que los crímenes más lucrativos, eran el narcotráfico, los estupefacientes, la trata de personas, que son hechos realmente graves, pero hoy lo supera el cibercrimen, por la rentabilidad de ganancia generada, de una forma muy fácil, solo ocupa una computadora, conectarse al ciberespacio y encontrar a las víctimas en la trampa cibernética.

Luego, se le unen factores como el anonimato, la complejidad las investigaciones de dar con el responsable, así como la falta de tipificación penal de los delitos informáticos en los diferentes países, hacen que esta tendencia criminal, sea hoy más común que de lo que se hubiese imaginado.

A esta tendencia criminal realmente, no se le está dando la importancia que merece, pues cada vez son más quienes se hacen dependientes de la tecnología, y ello hace que sean aún más vulnerables a un ciberdelito.

No siempre el ciberdelincuente, necesariamente va ser un hacker que es el sujeto con un conocimiento especializado, sino que cualquier persona con un conocimiento promedio en el uso de las tecnologías puede convertirse en un delincuente informático, y esto implica que las empresas sean víctimas corporativas de sus propios empleados. Esto hace notar que más bien siempre se habla del hacker como el sujeto responsable de las fechorías tecnológicas, pero no es el único capaz de delinquir en la vida cibernética, por ello se debe abrir la mente, en ese sentido.

Dada la relevancia que merece la ciberdelincuencia, el suscrito se avocó a realizar este proyecto de investigación para determinar si Costa Rica es capaz de brindarle a los ciudadanos una respuesta judicial efectiva cuando está frente a un delito informático.

1.2. FORMULACIÓN DEL PROBLEMA

¿Es suficiente el ordenamiento jurídico costarricense para enfrentar los fenómenos de la ciberdelincuencia?

¿Desde la perspectiva criminalística las autoridades cuentan con las técnicas y mecanismos efectivos para la obtención de elementos probatorios, ya que este fenómeno del cibercrimen depende de la cooperación internacional para la investigación?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

Para Guanipa (2008)

“los objetivos de investigación son las metas, propósitos o fines trazados por el investigador en concordancia con los aspectos que desea verificar y descubrir”

Según Ramírez (1996), “Los objetivos de investigación son metas que se traza el investigador en relación con los aspectos que desea indagar y conocer. Estos expresan un resultado o producto de la labor investigativa."

1.3.1. Concepto de Objetivo General

Según Arias (2006), un objetivo general expresa "el fin concreto de la investigación en correspondencia directa con la formulación del problema". (p.45)

Por su parte, Flórez y Tobón (2003),

> los objetivos están directamente relacionados con los tipos de conocimientos
> que se pretenden alcanzar en relación con las preguntas que constituyen el problema de investigación.

Herrera (2006),

> El objetivo es la categoría que refleja el propósito o intencionalidad de la investigación (el para que), lo que debe lograrse, de modo que se transforme el objeto y se solucione el problema. El objetivo expresa los límites del problema y orienta el desarrollo de la investigación al precisar que se pretende, por tanto, el título del proyecto de investigación o trabajo científico debe surgir del objetivo del para qué. (p.95)

1.3.2. Objetivo General de la investigación

Determinar la efectividad o la ineficacia con que cuentan las autoridades competentes para solicitar y recabar evidencia digital en el exterior con relación a los proveedores de servicio alojados en otros países, para tener una tutela judicial efectiva.

1.3.3. Objetivos específicos

Según (Álvarez Venegas, Paredes Hernandez, y Arteaga Pérez), (2015), indica que

"los objetivos generales dan origen a objetivos específicos que indican lo que se pretende realizar cada una de las etapas de la investigación. Estos objetivos deben ser evaluados en cada paso para conocer los distintos niveles de resultados". (p.17)

Sampieri (2014),

> Los objetivos deben expresarse con claridad y ser específicos, medibles, apropiados y realistas.

Para Tamayo (1994), hace referencia que los objetivos en una investigación son los enunciados claro y preciso de los propósitos por los cuales se lleva la investigación, de manera que, el objetivo del investigador es llegar a tomar decisiones y a desarrollar una teoría que le permita garantizar y resolver en la misma forma, problemas semejantes en el futuro”.

1.3.4. Objetivos específicos de la investigación

- **Explorar la totalidad de leyes y normativas existentes para determinar a ciencia cierta la carencia del delito Hacking.**

- **Realizar un análisis del derecho comparado en la región de Latinoamérica y España en relación con la tutela de ciberdelitos dados.**

- **Desarrollar un análisis de los mecanismos legales que poseen las autoridades competentes para la consecución de solicitar prueba al exterior a la luz de las distintas normativas y la posible aplicación de la Teoría de la prueba espuria.**

- **Determinar los instrumentos de investigación informáticas que posee la entidad investigadora en Costa Rica, para la recolección de prueba digital en la lucha en contra de la ciberdelincuencia, junto con las limitantes que cuenta la Policía Judicial.**

1.4. ALCANCES Y LIMITACIONES

1.4.1. Alcances

Esta investigación abarcará la totalidad del marco normativo del Estado Costarricense, considerando además los Convenios Internacionales para la prevención de los hechos delictivos, la amplitud de Tratados Internacionales para la asistencia internacional en materia penal, como también el procedimiento de las autoridades competentes. Así como la comparación de la regulación internacional en relación con los delitos informáticos y sus posibles adaptaciones al bloque de legalidad costarricense vigente.

También comprenderá el análisis de las distintas herramientas que posee el Organismo de Investigación Judicial para la prevención, detección y recaudación de prueba digital correspondiente a delitos informáticos que se dan en nuestro país, así como el análisis jurisprudencial por nuestros altos Tribunales de Casación y su posición al respecto, además como un hecho relevante se analizarán las estadísticas de cuáles son los casos más usuales en la lucha contra la ciberdelincuencia.

1.4.2. Limitaciones

La presente investigación no incluye ni va existir un estudio contable con respecto a las lesiones al patrimonio de los sujetos o empresas víctimas del hampa informático, y ni siquiera un cuadro comparativo que permita observar el aumento de flujo de información en el internet o que este almacenada en las distintas bases de datos, simplemente se va limitar a las incidencias que suceden en la esfera jurídica de la colectividad.

CAPITULO II: MARCO TEÓRICO

2.1. CONTEXTO HISTORICO

2.1.1 Raíces de la delincuencia cibernética

Dada la cibercriminalidad y sus repercusiones en el mundo económico de las empresas y de los ciudadanos, se debe recalcar que este fenómeno de las nuevas tecnologías (TICS), viene desde hace mucho tiempo desde la creación del internet, en conjunto con la aparición del malware o virus con fines maliciosos.

El inicio de esta cibercriminalidad, se dio por distintos estudiosos como Von Neumann que, en el año 1949, se encontraba escribiendo un libro sobre la Teoría y Organización de Autómatas Complejos, se basaba en que debía de existir una un artefacto tecnológico que pudiese reproducir programas con la capacidad de dominar el control de otros programas con la misma estructura. Bajo esta estructura quería que el virus tuviera efectos reproductivos en otro computador.

En 1970 el Doctor Gregory Benford, publica en una revista Venture Magazine la idea de un virus y la forma de eliminarlo a través de una vacuna, este se considera como el primer virus y tuvo la capacidad de infectar máquinas IBM 360 en una red que se llamó ARPANET, siendo necesario una forma de eliminarlos, por ello se creó un programa que se llamó Reaper, el cual fungía como un antivirus, actual predecesor de cómo combatirlos actualmente. En 1985,

el estudiante Cohen termina su doctorado enfocado en los Programas Auto-duplicadores, donde lleva intrínseco la definición de virus por primera vez y lo cataloga como “Programa que puede infectar a otros programas incluyendo una copia posiblemente evolucionada de sí misma”, por cierto, como hechos notorios indica la forma que se puede detectar un virus como, por ejemplo: detección por apariencia, por comportamiento, por evolución a otros virus, por engaño. En virtud de lo anterior, este estudioso se cataloga como el Padre de los Virus, quien a través del estudio de los algoritmos pudo determinar a ciencia cierta la técnica de los antivirus de hoy en día. A través de diferentes maneras Cohen podía establecer como distintos parámetros de detección de un virus como lo son: Por la apariencia, por el comportamiento, por la evolución de los virus de otros virus ya conocidos y por mecanismos de engaño. (Laboratorio de ESET Latinoamérica, 2012).

La cibercriminalidad se caracteriza por avanzar todos los días, no es un fenómeno que se queda estancado, por eso otros estudiosos, entre ellos: Tom Duff empezó a probar unos scripts en un sistema informático para su infección de virus en el computador, pero no tuvo esos efectos deseados, luego de las probanzas decidió en 1989 publicar un artículo del cual se denomina “Experience with viruses on Unisex Systems” del cual demostraba que podría infectar archivos ejecutables, sin modificar el sistema unix y que los virus 331 bytes se guardaban en ejecutables de 331 bytes.

Durante los años 1988, Adleman redactó un artículo “An abstract theory of computer services”, en donde era la primera vez que se incluía una definición sobre el termino Troyano, que al final de cuentas lleva el nombre por aquella gesta histórica de los griegos, donde de forma inocente logran entrar al sistema informático, sin embargo, dentro de ellas contiene maleza cibernética, y que hoy es una táctica infalible utilizada por los hackers para dañar los archivos de la computadora.

En los años 1986, se logró detectar la primera epidemia de virus en contra de los computadores IBM, esta se denominó Brain, sus fundadores fueron pakistaníes la función era infectar la zona de arranque, y cambiaba el nombre del disco, que al final simplemente según dicho de ellos era un experimento antipiratería.

Luego, el 02 de noviembre del año 1988, Robert Tappan Morris, creó un gusano de reproducción masiva, se colapso el 10% de Arpanet (era el internet en dicho contexto histórico), con ello este malware veía una vulnerabilidad en los sistemas operativos de Unix, por ello fue llevado a juicio por el delito de fraude y engaño condenado por la Corte Federal de Syracuse de New York, a tres años de libertad condicional y una multa de $10.000,00 y 400 horas de servicio comunal, esta fue la primera vez que existió una condena por un delito informático en Estados Unidos.

A nivel nacional, propiamente en los años ochenta aumentó la cantidad de denuncias por fraude informático, los ciberdelincuentes a través de los cajeros automáticos retiraban dinero proveniente de una tarjeta de débito o crédito robada, sin embargo, no existía ninguna sanción penal, pues Costa Rica no tenía ninguna regulación específica, sobre los delitos informáticos en ese entonces.

En el año 1997, surgió algo novedoso que a través de un correo electrónico podían enviar documentos infectados por MSmail, de igual manera los virus macro siguen creciendo en el año 1998 y tenían la posibilidad de infectar tres aplicaciones de Microsoft Office: Word, Excel y Power Point. De forma posterior en el 1999, apareció el virus Melissa en donde se enviaba un archivo adjunto que decía “No abra mensajes de personas desconocidas” y esto se daba en el Word 97 o 2000 en donde el virus iniciaba su maleza y luego abría Outlook, y se enviaba de forma automática los cincuenta contactos de la libreta, el fin era que recibieran el documento infectado para que de esa manera llegara la propagación, esto provocó grandes pérdidas económicas.

En el año 2003, aparecen los Botnets que en si informáticamente son redes zombie y que en si es una herramienta, la cual puede ser utilizada con diversos fines como lo son: Distributed Denia lof Service Attacks, Distribucion de Spam, Phishing, Escuchas de trafico de red, keylogging, distribución de malware, abuso de publicidad, robo masivo de datos, y es que son tan efectivos que pueden inhabilitar cualquier sistema de seguridad como firewall o un antivirus, vale la pena indicar que en el 2004 apareció el primer troyano para Mac Os X. En el 2005,

existe un cambio de tendencia se deja lo que son los virus y ahora lo que vale la pena son los gusanos y troyanos, siendo lo más rentable, de los cuales se distribuyen por spam y roban información relacionada con transacciones comerciales, como un nuevo método comienzan los phishing con versiones Qhost en donde mediante un Troyano se redirige al usuario hacia web falsa. (Laboratorio de ESET Latinoamérica, 2012)

En el 2008, con la aparición de las redes sociales, se empieza a ser víctima de códigos maliciosos, y en ese entonces fue el inicio para que hackers crearan perfiles falsos con fines delictivos. Luego con la aparición de los anuncios en redes sociales, se hizo viral, pues se ingresa al anuncio y cuando se da cuenta ya el computador está infectado por un malware que se escondía a través del anuncio. Estas conductas son del año 2008, que aún siguen sucediendo de forma muy común, como la suplantación de identidad, y la infección de malware.

De todo este apartado, se determina que el inicio de la cibercriminalidad se encuentra aparejado por la creación del Internet y los malware, que de una manera vinieron con el fin de infectar las máquinas de virus, como un medio de delincuencia informática, la cual sigue afectando a miles de usuarios on line.

2.1.1. Lucha contra la ciberdelincuencia a nivel del Consejo de Europa.

Por el carácter transfronterizo que tiene la delincuencia informática y por las repercusiones a nivel mundial DE este fenómeno, el Consejo de Europa adscrito a la Unión Europea, decidió ser el foco central para la lucha en contra de los ciberdelitos.

En el año 1997, los estudiosos Sieber, Kaspersen, Vanderbergue, Stuurman realizaron un informe denominado Los aspectos legales sobre el delito informático y la seguridad, para la conferencia de la Comisión Europea y del Consejo de Europa, realizada en Luxemburgo, que se discutía si existía algún avance en cuanto a la cibercriminalidad a nivel internacional y se buscó estandarizar una política penal en común de los Estados Miembros de la Unión Europea en contra del cibercrimen.

Luego, una de las iniciativas que impulsó el Consejo de Europa en relación con la lucha contra la delincuencia informática, fue la Decisión del Consejo del año

2000, donde rechazaba la pornografía infantil en Internet, por ser un delito tan detestable.

Dado el fenómeno de las nuevas tecnologías que afecta cientos de cibernautas, el Consejo de Europa, decidió crear un grupo de personeros especializados para crear una herramienta internacional, la cual permitiera a todos los países tener una política penal común en contra de la ciberdelincuencia, por ello se centraron en ciertos aspectos medulares como la parte sustantiva, la procesal, la cooperación internacional, bajo todo este enfoque realizaron un borrador para que tuviera un apoyo fuerte de los posibles países firmantes.

.

Dentro del procedimiento institucional que debió seguir el actual Convenio de Budapest, tuvo un arduo trabajo del Comité, en donde más bien los países negociadores los alentaban a continuar con la redacción, pues vendría a ser una gran herramienta para luchar contra el cibercrimen, y reconocían los Estados al Comité la necesidad de un sistema de cooperación internacional ágil, luego de múltiples reuniones con los Estados Miembros de la Unión Europea expresaron su apoyo al documento, sin embargo aún faltaban tres reuniones adicionales para finalizar el documento explicativo del Convenio de Budapest.

Posteriormente, en octubre del 2000, el Comité de Ministros le solicitó a la Asamblea que rindiera un dictamen sobre el Borrador del Convenio, no obstante, una parte del convenio no fue aprobada, por ello se le consulto a los demás Estados de la Unión Europea su parecer por las nuevas modificaciones del

documento, esto con el fin que tuviera un mayor apoyo, y más bien resultó muy útil.

Una vez que se revisó el Convenio con las modificaciones, se procedió con la aprobación del mismo, en la 50ª sesión plenaria en junio del 2001, y luego en proceso de firmas de los Estados.

Esta herramienta es un instrumento internacional, fue firmado en Budapest el 23 de noviembre del 2001, entro en vigor en el 2004, inclusive se permitió la adhesión de Estados no miembros del Consejo de Europa (Canadá, Estados Unidos, Japón, Sudáfrica, se han adherido), y actualmente Costa Rica que ya ratificó el convenio en julio 2017.

Sin lugar a duda, el Consejo de Europa ha mostrado un interés en animar a los estados miembros y terceros países para que lo ratifiquen, ya que se tocan términos muy novedosos, como datos informáticos, proveedor de servicios, datos de tráfico, que vienen a luchar en contra de la ciberdelincuencia. (Anguita, 2017)

El Convenio de Budapest trae múltiples beneficios aparte de lo normativo, pues el Consejo de Europa se comprometió a realizar constantemente capacitaciones a todos los Policías, Fiscales, Administradores de Justicia, para que estén

debidamente actualizados con las nuevas herramientas de los delincuentes informáticos.

En el 2004, en el Parlamento Europeo y en el Consejo de Europa, nació un Reglamento en donde se fundía la Agencia Europea de Seguridad de las Redes y la información, con el fin de garantizar un nivel efectivo y elevado de ciberseguridad, como medida de prevención de los delitos informáticos.

El Parlamento Europeo a través de la Directiva 2011/92/UE tomaron la iniciativa de crear otro instrumento internacional para la lucha en contra del abuso de menores por internet, la explotación sexual de menores y a la pornografía infantil, ya que es un tema muy repudiable en la sociedad, pues, se ven casos de videos con fines eróticos en donde participan niños de un año o hasta menos. (Anguita, 2017).

Un arma clave sería el nacimiento del Centro Europeo de Ciberdelincuencia (EC3) el día 11 de enero del 2013, quien se encuentra adscrita a la Oficina Europea de Policía (Europol) donde su principal objetivo será brindar la totalidad de conocimiento como centro de información y una fuente de apoyo importante para los operativos forenses, y crimen organizado. Los objetivos del EC3, definen el Consejo de Europa, (2013) como:

> . Además, prestará apoyo operativo a los países de la UE (por ejemplo, contra la intrusión, el fraude, el abuso sexual de menores en Internet, etc.) y aportará conocimientos técnicos, analíticos y de peritaje forense de alto nivel en el marco de investigaciones conjuntas. (p.1)

Véase que la promulgación del Convenio fue hecha en Europa, es decir solo aplicaba para países europeos, sin embargo, por la naturaleza del cibercrimen que es transfronterizo, decidieron invitar a firmar países no miembros de la Unión Europea como Costa Rica, a formar parte del Convenio de Budapest.

2.1.3. Costa Rica como país vanguardia a la luz del acontecer histórico a nivel de derecho penal informático nacional.

Siendo que la cibercriminalidad no es un fenómeno tan antiguo, la Legislación Costarricense, anteriormente no contemplaba ningún delito informático, pues no existía en ese entonces necesidad que el Código Penal fuese reformado, sin embargo, con el transcurso del tiempo, el desarrollo de las nuevas tecnologías, la aparición del Internet, hizo necesario que nuestro país, se fuera adaptando a las conductas ilícitas que sucedían en la convivencia social, y estas adaptaciones se decían dar a través de las Reformas al Código Penal. Por esa razón, en este capítulo se hará una reseña histórica de la evolución que ha tenido el Código Penal referente a los delitos informáticos.

Anteriormente el Código Penal que estuvo vigente fue el del año 1971, donde no existía ningún tipo penal sobre Delitos Informáticos, pues en dicho momento, el Legislador no consideró oportuno implementar los ciberdelitos, pues, aún no se daban en el país, conductas delictivas a través de un computador.

Lo único que se podía encontrar referente a los delitos informáticos, en ese momento se ubicaba en Leyes Especiales como la Ley General de Aduanas el ordinal 221 y 222, que entró a regir en noviembre de 1995, luego en el Código de Normas y procedimientos Tributarios, la tutela de ciertas actuaciones delictivas informáticas por los artículos 94, 96, 96, 97, que fueron implementados el 03 de agosto de 1999.

Por la globalización, donde se depende de un dispositivo móvil, de un computador, cada día que pasa la sociedad es mucho más tecnológica, y esto la convierte en una Sociedad de Riesgo, por estar conectados dentro del ciberespacio.

Posteriormente, en el año mil novecientos noventa y ocho, salió a la luz pública que ciertas personas se encontraban realizando un desfalco con las placas, fraudes registrales del Registro Nacional de la Propiedad y claras violaciones a Ley de Derechos de Autor, por esa razón los ciberdelitos iban en aumento sin una debida regulación punitiva, pues el Código Penal vigente era del año 1971 que no contenía ningún delito informático tutelado.

Y así fueron aumentando las actuaciones delictivas, siendo que para el año 2001, el periódico La Nación, le indica a la ciudadanía de cuan frecuentes son los delitos informáticos y la carencia de una legislación conforme. (Lemaitre, 2010)

Por esta razón, el Parlamento decidió presentar un Proyecto de Ley número 14097 que reformará el Código Penal en cuanto a la tutela de los delitos informáticos. En donde únicamente se implementaron tres artículos al Código Penal adicionado por la Ley Numero 8184 que entro a regir el 24 de octubre del 2001, y que dice así:

1) Artículo 196 bis.- Violación de comunicaciones electrónicas Será reprimida con pena de prisión de uno a cuatro años la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus mensajes de correo electrónico o cualesquiera otro tipo de telecomunicación de tipo remoto, documentos magnéticos, intercepte sus telecomunicaciones, o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación telemática. La misma pena se impondrá al que, sin estar autorizado, accede, se apodere, utilice, modifique o altere, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o

> privado, ya sea en perjuicio del titular de los datos o de un tercero. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
>
> Será castigado con las penas de prisión de uno a tres años, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior. Si los hechos descritos en los párrafos 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá pena de prisión de dos a seis años. (Ley N° 8184)

De la redacción del tipo, se desprende que deja al criterio del juzgador determinar qué tipo de objeto incurriría en la conducta, pues indica de cualquier tipo de telecomunicación de tipo remoto, documentos magnéticos, el legislador no fue especifico y da la oportunidad de una segunda valoración. Esta falencia del legislador, a la hora de redactar la normativa, es normal, ya que, si se contextualiza en la época del 2000 en Costa Rica, en donde este proyecto de ley era la primera iniciativa referente a los delitos informáticos, imagínese que esta rama del derecho penal es muy técnica y si no se cuenta con la suficiente experiencia o conocimiento puede acarrear carencias en la técnica legislativa.

Después de un análisis minucioso del tipo, se observa que el legislador en dicho momento, omitió la regulación de agravante cuando se trate de un funcionario público.

Siendo que los ciberdelincuentes, conocen lo que están haciendo, atina el legislador al imponer la conducta dolosa.

2) “Artículo 217 bis. - Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influyera en el procesamiento o en el resultado de los datos de un sistema de cómputo, mediante programación falsa, utilización de datos falsos o incompletos, utilización indebida de datos o cualquier otra acción que influyere sobre el proceso de los datos del sistema. (Ley N° 8184)

En relación con el sujeto activo, solo sanciona a cualquier persona física, omitiendo imponer una agravante al funcionario que con mucha más razón debió de ser implementado en la redacción, pues en la calidad de servidor público, tiene a disposición datos de miles de costarricenses en razón del puesto ocupado, por ende, debió tutelarse, y no caracterizarse por ser un delito común.

El termino correcto es el de estafa informática, ya que se lograría circunscribir de una mejor manera el campo de acción, pues fraude informático, es muy amplio y se incluyen conductas que no propiamente se relacionan a específicas como la Estafa. (Chinchilla, 2004)

Esta particularidad del fraude informático conllevó a una serie de impunidades, como lo indica la Sala Tercera de la Corte Suprema de Justicia (2006) señala:

> A juicio de esta Sala, la conducta tenida por probada – sustracción de la tarjeta de débito, obtención de la clave de ingreso, y uso de la tarjeta para conseguir en el cajero automático, dinero de la cuenta de la ofendida –, no es propia de dicha ilicitud, en vista de que P no manipuló los datos del sistema, ni influyó en su procesamiento. Como se señaló en un caso similar: “En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin; como medio en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal). “Por una parte, el National Center for Computer Crime Data indica que “el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes”. De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el “delito informático es toda conducta ilegal, no ética o

no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos". Asimismo, William Cashion – estadounidense experto en informática – señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología" (Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27). Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático. De acuerdo a la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas que han de incidir en el proceso de los datos del sistema. Influir en el procesamiento o resultado de los datos será manipular la información, alimentar el sistema de forma irregular, actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Por ejemplo, en el proceso de pagar el salario a los empleados habrá una serie de pasos por seguir, que, si alguno se altera fraudulentamente, incidirá en el resto del proceso. El usuario aparece al final de ese proceso, y en términos generales, no lo puede modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la

> destreza en el manejo de los sistemas informáticos, o una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas ventajas. Por estos aspectos son considerados “delitos de cuello blanco”. Esto por cuanto, además de la tecnicidad en el manejo de los sistemas, éstos se encuentran protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos. Como se observa, el delito de fraude informático requiere algún manejo de los datos, o los programas, que afecta el proceso de los datos del sistema. Por su parte, la conducta tenida por acreditada, en el caso en estudio, es el apoderamiento ilegítimo de dinero ajeno, utilizando la tarjeta original, por medio de un ordenador, pero sin modificación, ni alteración de la información que éste contenía, de modo que indujera a error en el procesamiento o el resultado de los datos del sistema. La acción realizada es la misma que hubiera hecho la titular de la tarjeta de débito, para obtener el dinero, por lo cual la conducta tenida por cierta no se adecua al tipo penal considerado por el Tribunal.

En la mayoría de los casos que se dieron en esa época, cuando los delincuentes tenían en su posesión una tarjeta de débito ajena, procedían con la sustracción del dinero, los jueces consideraban que la conducta no se ajustaba al Fraude informático, pues el delincuente, no manipulaba, no influía en el procesamiento de datos, ni tampoco inducia error al cajero, pues es la misma información que el titular hubiese puesto en el cajero. Por la mala redacción y poco conocimiento de los legisladores, pasaba esta situación que era algo muy común.

3) Artículo 229 bis. - Alteración de datos y sabotaje Informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accesare, borrare, suprimiere, modificare o inutilizare sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpeciere o inutilizare el funcionamiento de un programa de cómputo, una base de datos o sistema informático, la pena será de tres a seis años de prisión. En caso de que el programa de cómputo, base de datos o sistema informático contenga datos de carácter público, se impondrá pena de prisión de hasta ocho años. (Ley N° 8184)

De un estudio de la numeración el Legislador incurrió en un grosero error legislativo, ya que el 229 bis ya se encontraba tipificado por el Abandono dañino de animales, y mediante el Voto de la Sala Constitucional del 2007-18486, decretó la inconstitucionalidad de dicho artículo. (Sala Constitucional, 2007)

Del análisis detallado de esta reforma al Código Penal que entro a regir en el año 2002, del todo no cumplieron con las expectativas brindadas, ya que era un proyecto piloto, pues en el país, nunca había existido una iniciativa de ese tipo y era entendible que los legisladores no tuvieran la suficiente sabiduría.

Los delitos informáticos en Costa Rica fueron en aumento, pues 25 personas fueron estafadas por campañas publicitarias del Sistema Bancario Nacional y en donde brindaban datos confidenciales a los ciberdelincuentes por medio de correos electrónicos, esto según comunicado del Organismo de Investigación Judicial. (Prensa Libre, 2005)

Uno de los promotores de la siguiente reforma al Código Penal fue el Doctor Carlos Chinchilla Sandi en conjunto con la Comisión de Derecho Informático del Colegio de Abogados de Costa Rica, donde indicó que lo buscaron para redactar un borrador de ley avanzada, que marcara época, pues solo contaba con tres artículos relacionados a la ciberdelincuencia, y así fue como se le dio camino a la normativa vigente. (Chinchilla, 2015)

Esta sería la segunda reforma que sufrió el Código Penal a través de la Ley N°9048, donde se incluyó un nuevo capítulo de Delitos Informáticos y se agregaron unos delitos que no se habían contemplado antes, pues solo se contaba con tres artículos referentes a ciberdelitos, y por la expansión de las TICS, se requería de una reforma que se ajustara al contexto social donde se convive.

> Artículo 167.- Corrupción. Será sancionado con pena de prisión de tres a ocho años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. La pena será de cuatro a diez años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar. (Ley N° 9048)

Esta figura es conocida internacionalmente como Child Grooming, una persona mayor de edad que tenga conversaciones con fines eróticos en redes sociales con menores de edad, puede ir a la cárcel, siendo relevante para el Estado proteger el interés superior de los niños.

Artículo 196.- Violación de correspondencia o comunicaciones. Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino

documentos o comunicaciones dirigidos a otra persona. La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:

> a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.
>
> b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. (Ley N°9048)

Esta figura lo que viene a proteger es la intimidad de las personas, pues con las nuevas tecnologías, la privacidad va relacionada directamente con las comunicaciones en redes sociales, aplicaciones de conversaciones, y demás. Es un aspecto aún más amplio.

Para efectos de una mejor comprensión, se expondrá la definición de cada uno de los verbos mencionados, según indica la Real Academia Española (2017):

*Apoderar: Hacerse dueño de algo, ocuparlo, ponerlo bajo su poder.

*Modificar: Transformar o cambiar algo mudando alguna de sus características. Dar un nuevo modo de existir a la sustancia material.

*Alterar: Cambiar la esencia o forma de algo.

*Suprimir: Hacer cesar, hacer desaparecer.

*Intervenga: Tomar parte en un asunto. Sobrevenir, ocurrir, acontecer.

*Intercepte: Apoderarse de algo antes de que llegue a su destino. Interrumpir, obstruir una vía de comunicación.

*Utilice: Hacer que algo sirva para un fin.

*Abra: Descubrir o hacer patente lo que está cerrado u oculto.

*Difunda: Extender, esparcir, propagar físicamente.

*Desvié: Disuadir o apartar a alguien de la intención, determinación, propósito o dictamen en que estaba.

Todas aquellas situaciones que violentan la privacidad en las conversaciones, pueden ser sancionadas como delito, como lo es el hecho de abrir una conversación de whatsapp sin el consentimiento del usuario, así como el desviar, enviar un screenshot de una conversación a otra persona a lo cual no fue dirigido el mensaje de texto, dado el avance de las nuevas tecnologías (TICS) conlleva a una amplitud de conductas, que son sancionadas con cárcel y las personas no tienen conocimiento de las consecuencias que puede traer.

> Artículo 196 bis. - Violación de datos personales. Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera,

acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de cuatro a ocho años de prisión cuando las conductas sean descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) Cuando los datos sean de carácter público o estén contenidos en bases de datos públicas.

c) Si la información vulnerada corresponde a un menor de edad o incapaz.

d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona. (Ley N°9048)

Esta figura penal, busca proteger los datos personales de cada sujeto, que incluye, la etnia, tema salud, creencias, ámbito sexual, domicilio físico, el gps. Dado el avance que ha tenido el Internet, en nuestras vidas, y el gran panorama tecnológico que ofrece se podría considerar como delito, si un sujeto coloca un rastreador de ubicación (gps) en el vehículo, como una violación a un dato personal. Es muy amplio el fenómeno de las tecnologías, por ello hay que entenderlo de esa manera.

La intimidad o privacidad es un área restringida, de la cual surge el derecho a tener una vida privada sin intromisión, curiosidad, vigilancia, y espionaje. Este delito informático consiste en la violación de la intimidad de la vida personal y familiar, sea observando, escuchando o registrando hechos palabras, escritos o imágenes, valiéndose de instrumentos, procesos técnicos u otros medios. También se podría tipificar como delito el que organiza, proporciona, o emplea indebidamente un archivo con datos referentes a las convicciones religiosas, políticas o a la vida íntima de las personas. (Centro de Información Jurídica, 2006)

> Artículo 214.- Extorsión. Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero. La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica. (Ley N°9048)

Esta figura penal se conoce como Sexting, donde un sujeto aprovechándose de las imágenes, fotos con fines eróticos que tienen en su mano, pide a cambio una cierta cantidad de dinero a la víctima para que no difunda el material sexual que tiene en su poder el ciberdelincuente. Realmente, este delito también se denomina como Porno-Venganza, pues los exnovios se aprovechan de los amoríos que tuvo con su pareja, y las fotos intimas que tiene el exnovio, pues, tenían una relacion amorosa, y como la misma no terminó bien, busca sacar provecho extorsionando a la exnovia, afectándole en su vida cotidiana, familiar, laboral. Es una conducta reprochable, pues llega a cambiarle la vida a la víctima, si el ciberdelincuente publica las fotos intimas.

El desarrollo de las nuevas Tecnologías de la Información y la Comunicación (TIC), sumadas a los dispositivos electrónicos para la producción de material audiovisual inmediato, ha favorecido el uso de nuevas prácticas y conductas en los espacios de la intimidad sexual, de las que resultan imágenes o videos que son el resultado de un acuerdo entre las partes involucradas, pero reducidas al espacio de confianza/privacidad en que fueron obtenidas. Muchas de estas conductas devienen en situaciones impensadas para quienes la produjeron o consintieron. Tal es el caso de algunas personas que motivadas por represalia, resentimiento, extorsión, venganza o sentimientos de animosidad respecto de ex sus parejas o relaciones ocasionales de intimidad suben el ciberespacio imágenes y/o videos que atentan directamente con la libertad, la privacidad y

dignidad de las personas. A esta práctica de la conoce con el nombre de pornografía de venganza. (Buompadre, 2017)

> Artículo 217 bis. - Estafa informática. Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.
>
> La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. (Ley N°9048)

Anteriormente, se daba la problemática con este tipo penal, que los Tribunales de Justicia, aplicaban el delito de Hurto Agravado, cuando el delincuente robaba una tarjeta de débito o crédito, sustraía del dinero cajero automático, sin embargo con el anterior delito de Fraude Informático, no se podía

aplicar, pues los jueces consideraban que el delincuente no está manipulando ni influyendo en el procesamiento de datos del cajero, ni tampoco está induciendo a error a las máquinas, pues ingresa los mismos que el titular de la cuenta, hubiese puesto.

Existía una gran problemática, por esa razón se hizo necesario una reforma al anterior delito de Fraude Informático, a llamarse Estafa Informática, incluyéndose en el tipo el termino de uso indebido de datos, pues, eso era lo que hacía falta de tipificar y que el delito no fuera impune, como pasaba anteriormente. Como bien lo indica el Tribunal de Apelación de Sentencia Penal (2016):

> Finalmente, también se debe subrayar que el tipo penal no solo contempla el uso de datos falsos o incompletos, sino también el uso indebido de datos, supuesto que se articula en este asunto, pues si bien la clave o PIN es la auténtica, la víctima nunca suministró a Alfaro Masis esa información y menos aún consintió su empleo. (p.4)

> Artículo 229 bis. - Daño informático. Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable. (Ley N°9048)

Esta figura penal viene a proteger la integridad de la información que este contenía en cualquier contenedor electrónico, computadora, dispositivo móvil, siendo que en esta nueva era de la tecnología, la información actualmente vale oro. A nivel corporativo, que a una empresa le borren toda la base de datos de los clientes, es un perjuicio enorme, por ello se tipifica el daño informático por la relevancia que tiene la información en esta nueva Sociedad Informática.

De la Mata (2009) refiere que:

> Pues bien, la definición de lo que se entiende por daño informático debe permitir incluir tanto la destrucción de sistemas informáticos completos como la de sus componentes concretos, ya sean equipos, datos, documentos o programas. Y, lo que conllevará no pocos problemas de tipificación, ha de abarcar tanto lo que es en sí la destrucción de tales elementos o su inutilización como la simple perturbación del funcionamiento del sistema completo o de alguno de sus componentes funcionales. (p.316)

> Artículo 288.- Espionaje. Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los

> medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado. La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación. (Ley N°9048)

Esta figura penal viene a proteger la confidencialidad de la información referente a la Defensa Nacional, Seguridad del Estado, en donde sanciona a los funcionarios públicos que revelen información por vías informáticas datos referentes a la Defensa Nacional, el Narcotráfico, Crimen Organizado, pues podrían comprometer la labor del Estado. Por ende, es estrictamente privado la información que conozcan los servidores públicos, en razón del cargo dentro de la Administración Pública. Como lo indica la Secretaria de la Corte Suprema de Justicia (2010):

> Se introduce una figura novedosa y muy actual dentro del ámbito de los delitos informáticos, referida no la simple conducta de espionaje, sino aquella que tiene relación con la realizada por medio de la utilización de los modernas tecnologías de la información y la comunicación (TIC), donde se obtenga, indebidamente, informaciones secretas políticas o de los cuerpos de policía nacionales, o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación, o afecte la luchas contra el narcotráfico o el crimen organizado. El tipo base se sanciona con prisión de 4 a 8 años, además se incorporan conductas agravadas, sancionadas

> con prisión de 5 a 10 años, cuando la conducta se realice mediante la manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación. (p.105)

> Artículo 229.- Daño agravado. Se impondrá prisión de seis meses a cuatro años:
> 6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos. (Ley N°9048)

El legislador debió de haber incluido este inciso 6 dentro del artículo 229 bis de Daño Informático, pues es un inciso de agravante, y por efectos de orden lo debió haber adicionado al artículo de Daño por vías informáticas, ya que tiene estricta relación con este.

> Artículo 229 ter. - Sabotaje informático
> Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático. La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones. (Ley N°9048)

Esta figura penal, viene a proteger el funcionamiento normal de un sistema informático, siendo que los hackers, tienen un arsenal de herramientas para atacar un sistema y convertirlo en un sistema sin funcionamiento, pues inclusive tienen la posibilidad de hackear la página a tal punto, que cada uno de los cibernautas cuando deseen ingresar a la página, les rechace el acceso, pues la página está denegada, es decir, ningún usuario podrá accesar.

Sección VIII. Delitos informáticos y conexos. Artículo 230.- Suplantación de identidad. Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se

> le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero.
>
> La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz. (Ley N°9048)

Esta figura penal es novedosa, pues, lo que pretende proteger es la identidad virtual de cada uno de los usuarios on line, dentro del ciberespacio, ya que el ciberdelincuente, puede ser infractor de una norma haciéndose pasar en la red con una identidad digital falsa, la cual permitiría ocasionar daños a terceros sin que el titular de la cuenta, tenga estricto conocimiento. Por ello se regula y de una forma atina el legislador.

Es necesario acotar la definición de los siguientes términos del elemento normativo como lo señala Visión Criminológica Criminalística (2013):

> Por ello se define suplantación como una acción y efecto de suplantar, y éste último se precisa de la siguiente manera: Expresión que se define como ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba como el término -suplantar- contempla dentro de su expresión al individuo como dueño de su propia idiosincrasia, donde de manera a nada se vislumbra la pérdida de uno de los derechos fundamentales como ciudadano, misma que ha sido disfrutada por alguien más que ocupa los rasgos distintivos ajenos para realizar

> actividades ilícitas. Ahora bien, la suplantación de identidad se define como "uso indebido de identificaciones personales e información confidencial y privada por medio de vías físicas, informáticas, electrónicas y de telecomunicaciones para ejecutar actividades ilícitas perjudiciales, aspecto que contempla diversas modalidades de la conducta antisocial y no parte únicamente de lo posiblemente tangible. (p.15)
>
> Artículo 231.- Espionaje informático. Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. (Ley N°9048)

Esta figura penal internacionalmente se denomina Spyware, donde el ciberdelincuente se aprovecha del cargo que ocupa en una empresa, con el fin de apoderarse de información estrictamente confidencial perteneciente a la empresa donde labora, un clásico ejemplo seria que un colaborador de la Coca-Cola se apodere de la receta secreta para la elaboración de la gaseosa, y se la transmita a la Pepsi. Se le conoce como un espionaje industrial, en donde se apoderan información corporativa, con un valor económico muy fuerte dentro del comercio.

Artículo 232.- Instalación o propagación de programas informáticos maliciosos. Será sancionado con prisión de uno a seis años, quien, sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red

informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.

b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.

c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.

d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii) Afecte el funcionamiento de servicios públicos.

iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.

iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático. (Ley N°9048)

Este delito de Instalación o propagación de programas informáticos maliciosos, pretende proteger el correcto funcionamiento de un sistema informático, pues, con la aparición de las nuevas tecnologías (TICS) hace posible que cualquier computador sea infectado con un virus, y que no permita el correcto funcionamiento de la máquina. Los virus tienen diversas funciones como su propagación en otro dispositivo, un clásico ejemplo, sería que, en un computador infectado de virus, el titular sin percatarse ingresa una llave maya usb al computador y lo infecta también, por ende, pierde todos los archivos. El malware posee diferentes formas de aplicación, una de las comunes es el caballo de Troya que hace semejanza a la gesta heroica de los griegos, en donde dentro de la carnada, está todo el contenido malicioso del programa informativo, el cual infecta el computador.

Se puede conceptualizar al virus como un programa informático capaz de autorreplicarse a través de la infección de otros programas mayores, que permanecen ocultos en un sistema hasta darse a conocer, en dicho momento

producen daños, problemas, molestias al sistema informático, y por ende al usuario. (De la Cuadra, 2002)

> Artículo 233.- Suplantación de páginas electrónicas. Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet. La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero. (Ley N°9048)

Esta figura penal internacionalmente se conoce como Phishing, que en si lo que busca es engañar a la víctima a través del envió de un correo electrónico, simulando ser un correo de un Banco, de Apple, y lo que pretende es que la víctima a través de ese engaño creado por el ciberdelincuente, entre en el link, ingrese todas las credenciales de autenticación, su contraseña, y con ello lograron el cometido. Normalmente cuando la víctima hace acceso al link, que el delincuente informático envía, ni siquiera se nota que es una página falsa, pues contiene el mismo logo del Banco, el mismo color de la página, ósea, todos los detalles que como cibernauta se le hace similar a cierta página, sin embargo, todos los detalles presentes en la página web, son más bien una artimaña tecnológica realizada por los hackers para que sean presas fáciles, y generen un lucro importante.

En donde se infiere que el phising consiste en una modalidad de estafa, este tiene como objetivo intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjetas de crédito, identidades, etc. En resumen, extrae todas las referencias posibles para después usarlas con fines fraudulentos. (Bolaños & Becerra, 2005)

> Artículo 234.- Facilitación del delito informático. Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos. (Ley N°9048)

Esta figura penal, viene a complementar los demás artículos, pues no solo se sanciona al ciberdelincuente, responsable del delito informático, también se sanciona a la persona que facilita por cualquier la realización de un ciberdelito, un clásico ejemplo, sería que un colaborador le brinde la contraseña de acceso de la página web del trabajo a un hacker, para que el ciberdelincuente, sustraiga toda la información contenida en la base de datos de la empresa y luego extorsione a los dueños de la empresa para que les devuelva toda la información sustraída.

Como puntos relevantes también, se implementaron el ordinal 235 y 236 del del Código Penal con relación al narcotráfico, crimen organizado y la difusión de información falsa, dentro de la tipificación de los delitos informáticos.

Para ir finalizando la evolución de la legislación costarricense, siendo que, en el año 2012, se implementaron la gran cantidad de ciberdelitos, durante el año 2013, la Asamblea Legislativa, presentó su tercer proyecto de reforma a la Legislación Penal a través del Proyecto de Ley N°18546, ya que los artículos contenían unos pequeños yerros, los cuales fueron subsanados en la Ley N° 9135.

2.2. CONTEXTO TEÓRICO

2.2.1. Conceptualización del Delito Informático.

Dada la influencia de las nuevas tecnologías (TICS), en la convivencia digital el ciberespacio, donde se navega ha sido un lugar en el cual los hackers se aprovechan de las vulnerabilidades de los sistemas operativos, carencia de una cultura de seguridad informática de los usuarios en line y demás factores que permiten ser una presa fácil para los delincuentes informáticos. Por esta razón, es relevante conceptualizar el concepto del delito informático en sus aspectos generales.

La informática dentro de su ámbito permite: una agilización en el cálculo del hombre, desarrolla una relevante asociación y a nivel de lógica, se dirige específicamente a la memorización, almacenamiento de datos, información, imágenes y audios, tiene la posibilidad de comunicar datos e información. (Chinchilla, 2004).

El concepto de delito informático (ciberdelito) se puede definir como aquella conducta ilícita llevada a cabo mediante la utilización de un sistema informático o que involucre un procesamiento automático de datos.

Sardana (1979), lo define como:

> 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. 53)

En ese sentido, la definición del delito informático debe ser lo más amplia posible, pues, como la tecnología avanza todos los días, cada día sale a la luz algo nuevo, ahora se habla de la Inteligencia Artificial, contratos inteligentes, el bitcoin, por esa sencilla razón, la conceptualización del ciberdelito, no puede ser tan específica, ya que no calzaría con las nuevas herramientas tecnológicas que nacen a través de un computador, de un software.

En consecuencia, los delitos informáticos tienden a dividirse bajo dos ópticas: como medio y como fin. Debe entenderse el ciberdelito como medio, cuando el delincuente informático utiliza el computador, software, dispositivo móvil, para poder llevar a cabo el ilícito, sería como el canal que debe atravesar el hacker para lograr el cometido, a modo de ejemplo el espionaje informático, el hacking que es el intrusismo informático, desviación de fondos a otra cuenta bancaria, estafa informática, intervención de las líneas de comunicación, suplantar la identidad virtual de una persona en redes sociales, el pichinga, Business Email Compromiso (BEC) y demás hechos que ponen al sistema informático como el método o medio del hecho delictivo.

Debe entenderse el delito informático como fin, cuando el criminal cibernético tiene como único objetivo el computador, es decir, ya no lo utiliza como herramienta, sino que ahora tiene la mirada exclusivamente puesta en la computadora, software a modo de ejemplo el sabotaje informático, destrucción de un programa, programación de instrucciones que provoquen un bloqueo total al sistema, secuestro de soportes magnéticos que exista información valiosa con fines de chantaje. (Téllez, 1996)

En otro orden de ideas, ciertos doctrinarios indican que el Derecho Informático no es una rama a la cual se le debe dar tanta importancia, pues para eso existen las figuras penales tradicionales, ya que incurrirían en una doble de tipificación de conductas que se puede aplicar a las ya existentes, y por esa razón, no le prestan la relevancia que merece. Champola (2003) señala:

> Los Delitos Informáticos, en su gran mayoría dependen, para su persecución penal de la correcta interpretación de la ley penal y de la toma de conciencia por parte de los jueces de que sólo nos encontramos ante nuevos métodos para estafar o para injuriar, pero en ningún caso ante nuevos delitos, ya que una postura semejante nos llevaría al absurdo de pensar, por ejemplo, que si mañana se pudiese quitarse la vida a alguien por medio de Internet habría que establecer una nueva figura penal ya que, el homicidio no estaría cubriendo esta posibilidad; cuando en derecho, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado

> corresponde la aplicación de la ley penal vigente y no se requiere de una nueva y específica. (p.17)

Con base en la postura del autor, se discrepa totalmente siendo que el Derecho debe de adecuarse a las nuevas conductas sociales que en esta rama particular se caracteriza por la aparición de las nuevas tecnologías (TICS) bajo este fenómeno, el cual vino a revolucionar el mundo entero, se está en una era de globalización innegable. Entonces bajo este concepto, aplicar las figuras penales preexistentes, las tradicionales, no tendrían ningún efecto, pues, incurre en atípica la conducta, por ello las legislaciones deben estarse actualizando periódicamente mediante las reformas de ley, para que se adecuen al contexto social correspondiente. En razón de lo anterior, esta nueva rama del Derecho Penal amerita mucha importancia, pues, engloba a toda la sociedad, a los profesionales y personas en general que viven en un mundo inmerso de las nuevas tecnologías (TICS).

Ahora bien, el criminal informático posee ciertas habilidades como un conocimiento promedio en el uso de las tecnologías, no necesariamente el ciberdelincuente siempre va ser un hacker, que posea un conocimiento especializado en el área, sino que de esta manera se amplía el horizonte, inclusive desde el ámbito laboral los propios colaboradores dentro de la organización corporativa pueden aprovecharse del cargo y las herramientas que poseen para la comisión del delito informático, a estos últimos se les denomina como delitos ocupacionales en el ámbito cibernético.

A nivel empresarial, cuando son víctimas de un delito informático, no presentan la denuncia correspondiente, ya que les da un temor inmenso que a raíz, del hacker, les vaya afectar de algún modo la reputación, la fama, la credibilidad con los clientes de la empresa, causaría más daño desde la perspectiva de la empresa que fueron víctimas de un ciberdelincuente que el daño en si cibernético, por ende, las pérdidas que tuvo la empresa producto del cibercrimen, se van directo a la cifra negra, esta es una estadística de pérdidas que han tenido las empresas a nivel mundial, pero que no han reportado el delito ante las autoridades competentes, por eso, se maneja como una información extraoficial.

La situación actual es que el grueso de los delitos informáticos no es descubierto o no son denunciados por los sujetos pasivos, por ello resulta imposible poder saber con certeza la verdadera magnitud de estos. Una de las posibles causas de la falta de denuncias reside en el temor por parte de empresas que hayan sido objeto de algún tipo de fraude informático de denunciar este tipo de infracciones por el posible desprestigio que esto pudiera ocasionar a la misma y las consecuentes pérdidas económicas y de imagen ante la sociedad, debiendo recurrir a la denominada como cifra negra para poder valorar las estadísticas sobre este tipo de conductas. (gallego, 2012)

2.2.2. Ciberdelitos y su Derecho Comparado en Latinoamerica y España.

2.2.2.2 MÉXICO

Dado que el cibercrimen trasciende fronteras, las legislaciones deben contar con un marco jurídico que pueda atender los delitos informáticos, por esa razón se da inicio con México, donde se analizará a través del Derecho Comparado con el costarricense la forma de regulación. En el Código Federal Mexicano correspondiente al Título Noveno se encuentran los artículos sobre Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática.

> **Artículo 210.** Se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que, sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto. (Código Penal Federal Mexicano)

De esta figura penal mexicana se observa que se tutela a través de una contravención, pues la sanción penal por imponer es trabajo comunal de

doscientas jornadas de labor social, no obstante, en Costa Rica la misma figura penal de Violación a la Correspondencia se sanciona con pena privativa de libertad y no como contravención como lo dicta el Código Penal Mexicano.

Pero que ha sido definitivo para prolongar la confusión. que hoy se vive es una falta de una técnica legislativa apropiada, falla que, unida al intervencionismo del Estado el que ha aumentado en los últimos tiempos en casi todos los países en aras del bien social, ha llevado a los legisladores a considerar, con su propio criterio, como conductas de peligro que no causan un daño real ni lesionan derechos particulares, deben ser delitos; y que conductas que fueron delitos y lesionan intereses particulares pasen a ser contravenciones, por ser consideradas menos graves. (Henao de Yepes, 2001,)

> **Artículo 211.** La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que presta servicios profesionales o técnicos o por funcionario o empleado público o cuando el secreto revelado o publicado sea de carácter industrial. (Código Penal Federal Mexicano)

En esta figura penal los legisladores mexicanos decidieron imponer una pena de multa y de inhabilitación, y no como lo establece el Código Penal

Costarricense, en donde la totalidad de delitos informáticos son penados con privativa de libertad. Luego, del tipo penal no se deduce claramente si se podría clasificar como un ciberdelito, pues no indica el legislador mexicano si la revelación o difusión se da valiéndose de una manipulación informática o tecnológica.

De dicho artículo del Código Penal Mexicano, el tipo penal carece de verbos como lo son el apoderamiento, la modificación, la interferencia, el acceso, copiar, transmitir, vender, comprar, difundir, como lo dictamina Código Penal Costarricense, pues, por la amplitud de las nuevas tecnologías (TICS) permite un sinfín de conductas que deben ser determinadas en las leyes.

> **Artículo 211 bis.** A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. (Código Penal Federal)

Dada la aparición de las nuevas tecnologías (TICS) que permiten un sinfín de conductas, se determina esta figura penal mexicana posee una escasez de verbos, pues para la revelación en el ámbito informático, se puede dar a través de diferentes maneras como apoderarse, alterar, abrir, entregar, vender, y no quedarse únicamente con la divulgación o revelación, que son términos muy amplios. El Código Penal Costarricense incluye dentro del tipo todos los verbos

que se indicaron, pues, es de suma relevancia, tutelar de una forma efectiva la intimidad de las personas.

.

> **Artículo 211 bis 1**. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. (Código Penal Federal Mexicano)

Que esta figura penal mexicana es escasa en cuanto a los verbos del tipo penal, pues el legislador mexicano debió de haber incluido verbos como la destrucción, alteración, entorpecimiento, inutilización, ya que son las vías informáticas más utilizadas por los ciberdelincuentes para que el sistema operativo, servidor, no llegue a funcionar adecuadamente, pues este delito informático, lo que trata de dañar es el normal funcionamiento del computador, en síntesis, convertirlo en inoperante.

Que por el auge que posee la tecnología en el sector público, en donde cada vez es más común, que el servicio público prestado a los ciudadanos es de forma virtual, el legislador mexicano debió de haber contemplado un supuesto de agravante cuando el Sabotaje Informático, realizado por el hacker tenga repercusiones en el servicio público brindado, como si lo tipifica el Código Penal Costarricense.

> **Artículo 211 bis 2**. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. Las sanciones anteriores se duplicarán cuando la

> conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes. (Código Penal Federal Mexicano)

Se podría utilizar la razón e interpretar que la protección se refiere a contraseñas, antivirus u otras medidas por medio de software, tendientes a negar el acceso tanto de personas como de virus, sin embargo al no especificar la norma, una puerta con llave o el simple apagado del equipo, podría bastar para cumplir la condición y si se recuerda que se trata de legislación en una materia en la que la libertad de personas están en juego, interpretaciones como la recién plasmadas deberían ser evitadas mediante técnicas legislativas correctas. (López & Torres, 2010)

> **Artículo 211 bis 3.** Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que, estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien, estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá, además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. (Código Penal Federal Mexicano)

Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. (Código Penal Federal Mexicano)

Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. (Código Penal Federal Mexicano)

Artículo 211 bis 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código. (Código Penal Federal Mexicano)

Artículo 211 bis 7. Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno. (Código Penal Federal Mexicano)

Siendo que se brindó el análisis comparado de la normativa relacionada con ciberdelincuencia en México, se da por terminado el apartado de la región mexicana.

2.2.2.3 Guatemala

Dado que se está realizando el análisis de la legislación en la región latinoamericana, es relevante hacer referencia de este país centroamericano con un desarrollo legislativo fuerte introduciendo al Código Penal Guatemalteco el Capítulo VII, titulado De los Delitos Contra el Derecho de Autor, la Propiedad Industrial y Delitos Informáticos.

> **ARTICULO 274 A**. Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos. (Código Penal de Guatemala, 2018)

> **ARTICULO 274 B**. La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras. (Código Penal de Guatemala, 2018)

Que de esta figura penal se determina que el legislador guatemalteco debió de haber incluido en el artículo 274 A, un supuesto de agravante cuando el registro informático que se destruya es insustituible e irrecuperable, pues, si lo que se pretende proteger es la información contenida en un sistema informático, contenedor eléctrico, debe de ampliarse el panorama, pues al estar frente a las nuevas tecnologías (TICS) permite que cualquier archivo sea borrado y a través de artificios tecnológicos, los cuales provoquen que el registro informático, nunca más se pueda volver a obtener. El Código Penal de Costa Rica, contiene regulado el agravante cuando sea información que no se pueda recobrar.

Luego del otro artículo 274 B, el legislador guatemalteco debió haber incluido dentro del tipo penal verbos como alterar, entorpecer, impedir, pues si lo que se pretende tutelar es el funcionamiento de la máquina, dispositivo y evitar de esta forma un Sabotaje Informático, debió haberse redactado de esa manera, pues el ilícito de sabotaje se puede dar de distintas vías, y no limitarse a las que están en este momento vigente. Que producto de la rentabilidad que genera el cibercrimen, es necesario tutelar no solo al autor material que realiza el ciberdelito, sino que también, existe la posibilidad que un tercero le cancele a un hacker una cierta suma de dinero para realizar el sabotaje, por ende, está ejecutando el delito por un

beneficio de un tercero. Este hecho que se acaba de indicar está regulado en el artículo 229 ter del Código Penal de Costa Rica.

> **ARTICULO 274 C.** Se impondrá prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales al que, sin autorización del autor, copiare o de cualquier modo reprodujere las instrucciones o programas de computación. (Código Penal de Guatemala, 2018)

Que el legislador guatemalteco debió haber incluido este tipo penal en una Ley especial de Derechos de Autor, como se encuentra tutelado en Costa Rica bajo la Ley sobre Derechos de Autor y Derechos Conexos N°6683, en donde contiene toda la normativa relacionada con infracciones a propiedad intelectual.

> **ARTICULO 274 D**. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.

Que del tipo penal que impuso el legislador guatemalteco, se determina la prohibición de crear una base de datos, pues puede afectar la intimidad de los ciudadanos, sin embargo realizando el análisis de un Derecho Comparado de Costa Rica, se posee más bien una Ley N° 8968 que regula a la Protección de la persona frente al Tratamiento de datos personales, y permite la creación de bases de datos publicas, privadas siempre y cuando se inscriba ante la Agencia de

Protección de Datos y Habitantes de Costa Rica (PRODHAB) en donde debe contar con todas las medidas técnicas para garantizar la seguridad de los datos personales

> **ARTICULO 274 E**. Se impondrá prisión de uno a cinco años y multa de quinientos a tres mil quetzales, al que utilizare registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica.
>
> **ARTICULO 274 F**. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.

Este artículo está mal redactado, tiende a punir actos preparatorios inclusive actos que tradicionalmente son impunes en el éter crimines, al hacer esto no solo permite imponer prisión por acciones muy poco lesivas, sino que podría provocar concursos aparentes con delitos como fraudes. Todas las acciones descritas en el

tipo es posible visualizarlas en contextos no lesivos y aun así punibles según el artículo. (López & Torres, 2010)

De esta manera, se concluye con el análisis de la legislación guatemalteca, y como punto adicional por la ratificación del Convenio de Budapest del Gobierno de Guatemala, en la lucha contra la ciberdelincuencia, el Consejo de Europa en conjunto con las autoridades competentes guatemaltecas, elaboraron una iniciativa de reforma al Código Penal, bajo las recomendaciones del Tratado Internacional.

2.2.2.4 Panamá

Que la legislación panameña actualmente cuenta con un marco jurídico contra la lucha de la ciberdelincuencia, de únicamente cuatro artículos dentro del Capítulo X bajo el nombre de Revelación de Secretos Empresariales, siguientes y concordantes. Derechos Digitales (2017) señala:

> Sin embargo, actualmente, el Código Penal vigente únicamente tipifica 2 conductas como delitos informáticos, y no incluye los delitos que se realicen por medios electrónicos. La construcción de políticas públicas y legislaciones, sustantivas y procesales, adecuadas a los estándares internacionales en materia de ciberdelincuencia es una

> urgencia en Panamá. Las entidades públicas que participan en los procesos de investigación penal y de otros sectores, como el sector privado y la comunidad técnica, deben buscar el desarrollo de capacidades para hacer frente en la lucha contra la ciberdelincuencia. Una reforma adecuada de este último permitiría que los mecanismos para la investigación penal aseguren la correcta guía y salvaguarda de los derechos humanos y garantías procesales reconocidos por tratados internacionales y la Constitución. (p.1)

> **Artículo 288.** Quien, para descubrir innovaciones o secretos de un agente económico, se apodere de datos, información, soporte informático, formula o informe, siempre que cause perjuicio a este, será sancionado con prisión de dos a cuatro años.
>
> La prisión será de tres a seis años, si el autor se apodera de los secretos de la empresa como servidor público, trabajador de la empresa o en virtud de la prestación de servicios profesionales.

Que de esta figura penal el legislador panameño impuso como verbo del tipo únicamente quien se apodere, es decir, que tenga a su disposición el contenido confidencial, sin embargo, debió de haber incluido verbos como vender, transmitir, pues se debe considerar que dicha información tiene un valor de comercio fuerte que debe ser visto de esa manera, como sucede en el Código Penal de Costa

Rica, el cual brinda un escenario de opciones que podría realizar el ciberdelincuente en el mercado.

> **Artículo 289.** Quien indebidamente ingrese o utilice una base de datos, red o sistema informático, sera sancionado con dos a cuatro años.

Que el legislador panameño sanciona con pena privativa de libertad el uso de una base de datos, sin embargo, en Costa Rica a través de la Ley N° 8969 de la Protección de Datos Personales, se permite más bien la creación de base de datos públicas y privadas en donde deben estar inscritas ante la PRODHAB, cumpliendo con los requisitos de la ley. Esta agencia se encuentra adscrita al Ministerio de Justicia y Paz en donde el fin primordial es velar que la autodeterminación informativa de cada ciudadano se cumpla, por ello el legislador panameño, no debe prohibir el uso de una base de datos, sino que debe establecer las medidas pertinentes para la regulación de los datos personales, como lo regula Costa Rica a través de esa ley especial.

> **Artículo 290**. Quien indebidamente se apodere, copie, inutilice o modifique, los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice, o impida su transmisión sera sancionado con dos a cuatro años de prisión.

Que el legislador panameño debió de haber incluido en el tipo penal sin la autorización del titular, pues si lo que pretende proteger es la intimidad del ciudadano, nunca va a existir una autorización para la lesión de ese derecho, por ello, debió de haberse establecido que el ilícito se da cuando no exista la autorización del titular, como lo tipifica el Código Penal de Costa Rica.

Artículo 291. Las conductas descritas en los artículos 289 y 290 se agravarán de un tercio a una sexta parte, si se cometen contra datos contenidos en bases de datos o sistema informático de:

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

También se agravará la pena en la forma prevista en este articulo cuando los hechos sean contenidos con fines lucrativos. Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del estado, según lo dispuesto en el Capítulo I, Titulo XIV, del Libro Segundo de este Código.

> **Artículo 292.** Si las conductas descritas en el presente capítulo, las comete la persona encargada o responsable de la base o sistema informático, o la persona autorizada para acceder a este, o las cometió utilizando información privilegiada, la sanción se agravará entre una sexta y una tercera parte.

En los dos últimos artículos, se tipifican las agravantes que se asocian directamente al capítulo de los delitos informáticos. Proyecto de Ley N° 558 de Panamá (2017), afirma:

> La República de Panamá, no escapa a esta realidad. Uno de los propósitos de este Proyecto de Ley, es regular a la luz de la ley sustantiva, la protección de la información y tipificar conductas delictivas, relacionadas a las nuevas tendencias que incluyen desde el acceso ilegal a sistemas informáticos, suplantación de identidad, interceptación ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de datos informáticos), extorsión. fraudes electrónicos, estafas, ataques a sistemas informáticos, ataques realizados por hackers, captura de datos bancarios (phishing. pharming), computadoras zombies (balnels), violación de los derechos de autor, pornografía infantil, pedofilia, denegación de servicios, ciberacoso (ciberbllllying y cibergraoming), 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 (correo basura), de ataque masivos a servidores de Internet y mediante generación de virus. (p.2)

Amén de lo anterior, la Procuradora de Panamá, presentó un Proyecto de Ley de Modificación y Adición al Código Penal relacionados al Cibercrimen bajo la Ley N°558 ante el Parlamento Panameño para que reformasen el Código Penal de Panamá, que aún no ha sido aprobado.

2.2.2.5 Colombia

Este país, tuvo su gran desarrollo normativo con relación con los delitos informáticos en el año 2009, en donde a través de la Ley N°1273, se modificó el Código Punitivo en dos capítulos: uno a través de la integridad de la información y el otro capítulo relacionado con los atentados informáticos. Alciver, Álvarez, Ortiz (2016) reseñan:

> No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de

clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según estadísticas, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos. De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado De la Protección de la información y de los datos que divide en dos capítulos, a saber: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y De los atentados informáticos y otras infracciones.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (Ley N°1273)

Que el legislador colombiano implementó esta figura penal que viene a tutelar es el acceso no autorizado, que no requiere de un daño palpable para su configuración, es decir, se podría decir que no es un delito de resultado como

ciertos autores opinan, que debe existir un daño tangible cuando se ingresa ilegítimamente. Posada (2006) define el hacking como:

> Arrogarse ilegalmente de forma no autorizada el derecho o la jurisdicción de interesarse o ingresar en un sistema informático o red de comunicación electrónica de datos, con la consecuente trasgresión de las seguridades dispuestas por el Web master o prestador del servicio al Web hosting u Owen, con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros. (p.11)

> Artículo 269 B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA
>
> INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor. (Ley N°1273)

Que el Legislador Colombiano, debió contemplar los componentes físicos o lógicos del mismo sistema, pues, si lo que pretender proteger es el funcionamiento de la máquina, debe ampliarse el panorama a todos los componentes del sistema

informático, como lo regula el Código Penal Costarricense a través del numeral 229 ter.

Este delito se relaciona con el uso de diferentes herramientas empleadas por un hacker o delincuente cibernético para interrumpir las funciones normales de un sistema, con el fin de conseguir un beneficio como robo o borrado de información o en algunos casos realizar un daño a gran escala, denegando los servicios de red o telemáticos, en donde la organización no tenga comunicación interna ni externa lo que implica pérdidas millonarias, esto se debe a la parálisis del normal funcionamiento de la empresa hasta lograr una solución que permita retomarla. (Sánchez, 2017)

> Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis a setenta y dos meses. (Ley N°1273)

Dado que en el Código Procesal Penal Colombiano establece la posibilidad de interceptación de datos informáticos, siempre y cuando sea autorizada por una orden judicial, por ende, se considera delito en Colombia a la persona que realice esta interceptación sin la debida autorización del juez, se sanciona con pena privativa de libertad, es decir, por el no cumplimiento del debido proceso conlleva

a esta sanción penal. En Costa Rica no permite la interceptación de los datos informáticos, pues, la Ley N° 7425 sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, únicamente establece la posibilidad de autorizar el registro de documentos privados.

> **Artículo 269 D. DAÑO INFORMÁTICO**. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley N°1273)

Que esta figura penal protege la integridad de la información, por ende, el legislador colombiano debió haber incluido dentro del tipo penal que si el ciberdelincuente se excede del permiso que el titular propietario de la información le concedió para destruir la información, incurre en este delito, como lo regula el Código Penal de Costa Rica en el artículo 229 bis, pues lo que pretendió tutelar el legislador costarricense es la voluntad del titular en el marco del uso discrecional de la información perteneciente a su persona. Que el legislador colombiano, omite establecer pena de agravante si la información que borro es de carácter irrecuperable, por ello es meritorio de una pena mayor por su condición y el daño causado al victimario.

Cuando se habla de daño a la información se debe tener en cuenta toda acción que afecte o vulnere la integridad de la información mediante el borrado, el deterioro, destrucción o alteración para cometer un ilícito que deje algún tipo de beneficio económico o de cualquier otra índole. Esta conducta delictiva es una de las comunes y no sólo se refiere a la información como archivos o el daño a aplicaciones, sino que también debe hacer referencia al daño que se pretenda materializar en contra de cualquier elemento lógico o físico que haga parte de un sistema (Sánchez, 2017)

> Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley N°1273)

Que el legislador colombiano omite establecer agravantes cuando el software malicioso afecte servicios públicos esenciales, en donde existiría un perjuicio a la sociedad por el no funcionamiento del software, a causa del ciberdelincuente, como lo regula del Código Penal de Costa Rica en el artículo 232 inciso II.

> Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga,

> compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique, o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Ley N°1273)

Que el legislador colombiano omitió imponer un agravante cuando la información vulnerada le corresponda al menor de edad o un incapaz, no se ven configuradas, pues, si lo que pretende proteger es la confidencialidad de los datos personales, se debió contemplar a las personas más vulnerables dentro un agravante, con una pena mayor. El Código Penal de Costa Rica lo regula en el artículo 196 bis inciso b.

> Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR
>
> DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia

> de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. la pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. (Ley N°1273)

Que el legislador colombiano lo que tutela es el Phishing, sin embargo, omite incluir dentro de tipo penal como víctima a las personas jurídicas, pues los hackers, tienen como presa principal a los Bancos, Empresas, ya que normalmente dentro del comercio electrónico fluyen grandes cantidades de dinero. En el artículo 233 del Código Penal de Costa Rica, se implementa como sujeto victimario a las personas jurídicas, cuando se captura información confidencial.

Este delito hace referencia al famoso Phishing y hace parte de los ataques de ingeniería social, los cuales se han perpetuado valiéndose de las vulnerabilidades no de los sistemas informáticos sino de los errores o fallos humanos, mediante los cuales logran conseguir datos personales que puedan servir para engañar y sustraer información. (Sánchez, 2017)

De esta manera se concluye con el análisis del Derecho de Comparado Colombiano, determinando las diferencias que tiene con el ordenamiento jurídico costarricense en relación con los delitos informáticos.

2.2.2.6 Argentina

Que este país sudamericano, cuenta con un marco jurídico contra la ciberdelincuencia que fue reformado por la Ley N° 26388, que entró en vigencia el día 25 de junio del 2008, en donde vino a reformar el Código Penal de la Argentina mediante el Capítulo III Violación de Secretos y de la Privacidad, donde se detalla.

ARTICULO 153. - Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena. (Ley N° 26388)

El artículo anterior procede a incluir las comunicaciones informáticas dentro de un tipo penal tradicional como lo es la interceptación de correspondencia, si bien la técnica parece acertada, pues como se ha venido repitiendo, no todos los delitos

que se valen de sistemas informáticos son merecedores de tipificación independiente, en muchos casos basta con utilizar tipos clásicos a los cuales por mayor seguridad jurídica deberán ser adicionados con esta nueva vía de comisión de delitos. (López & Torres, 2010)

> ARTICULO 153 BIS. - Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. (Ley N° 26388)

Que el legislador argentino implementó la conducta de Hacking, ya que el tipo penal contiene vocablos de acceder de forma ilegítima a un sistema informático o a un dato, siendo este delito de muy vieja data. Es atinado los supuestos de agravantes, pues, de acuerdo con las nuevas tecnologías (TICS), que vienen a incursionar en el servicio público prestado a la sociedad, así las cosas, se debe penar con mayor gravedad.

> ARTICULO 155. - Será reprimido con multa de pesos un mil quinientos a pesos cien mil el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.
>
> Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público. (Ley N° 26388)

De la lectura de este artículo se desprende, que no es posible determinar a ciencia cierta cuando el delito, causará un perjuicio a tercero, pues, es un hecho indeterminado. El Derecho Penal, al ser una materia tan odiosa, se requiere que el tipo penal sea lo más específico posible, pues como se sabe no se puede utilizar la analogía, ni que se pueda llevar a segundas valoraciones, sino que debe cumplirse necesariamente. El Código Penal de Costa Rica a través del artículo 196, estableció más bien que cuando la conducta produzca un daño a la intimidad de otro, se penará con privativa de libertad, por ende, el legislador argentino, debió haberlo redactado de otra forma para una debida comprensión.

> ARTICULO 157 bis. -Será reprimido con la pena de prisión de un mes a dos años el que:
>
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años. (Ley N° 26388)

Con relacion al artículo el legislador argentino lo reguló, como un delito de peligro abstracto y no de resultado. Siendo que más bien otros estudiosos indican, que al no existir ningún daño al acceso ilegitimo, no es posible considerarlo como delito, no obstante, se puede observar que el bien jurídico por tutelar es el acceso no autorizado, es decir, por el quebrando de las medidas de seguridad o credenciales de autenticación que se le colocan al sistema informático, y que violentan la intimidad del usuario y a partir de allí se configura, el ciberdelito, por esa razón, no se requiere que exista un daño a causa del acceso no autorizado. No es posible realizar el análisis de derecho comparado con este delito, pues Costa Rica, no contiene ningún artículo relacionado al hacking.

> ARTICULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
>
> 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (Ley N° 26388)

Que el legislador argentino debió haber incluido dentro del tipo penal, el termino influir, pues para realizar el delito por parte del hacker, no es necesario una alteración del funcionamiento normal del sistema informático, sino que únicamente se requiere que influya o incida en el procesamiento de datos, por ende, existe una mala praxis, en la parte técnica del delito. El Código Penal de Costa Rica a través del artículo 217 bis, regula de una forma practica la Estafa Cibernética, pues se llega a cumplir el delito, cuando exista una manipulación, cuando haga un uso indebido de datos o si más bien el hacker influye en el ingreso de datos y en el procesamiento.

Un clásico ejemplo de esto es la creación de empleados fantasmas a quienes el sistema deposita un salario sin significar que el sistema funcione anormalmente, por el contrario, el normal funcionamiento es necesario para el fraude. (López & Torres, 2010)

> ARTICULO 184. - La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes:
>
> Inciso 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público. (Ley N° 26388)

Que el legislador argentino no toma en cuenta que la gran mayoría de los delitos informáticos son realizados por los administradores de las bases de datos, o los encargados de dar soporte a la red en una empresa, por ende, se debió haber incluido dentro de los agravantes. En el Código Penal de Costa Rica, la gran mayoría de los ciberdelitos siempre existe una pena de agravante cuando realice el hecho delictivo el encargado de dar soporte a la red o servidores, es decir, los de TI.

2.2.2.7 España

Durante el año 2015, el Código Penal Español sufrió modificaciones relevantes en su tipificación, pues se vieron en la necesidad de la globalización y de los fenómenos planteados por las nuevas tecnologías (TICS), implementaron una serie de conductas delictivas en la esfera contra la ciberdelincuencia, y hoy, este país, se considera como un promotor de los ciberdelitos en Europa. Guardiola (2016) indica que:

> Esta nueva realidad ha hecho que se haya gestado toda una nueva categoría de nuevos ciberdelitos, bautizados como "delitos informáticos", que tienen como punto en común las Nuevas tecnologías como medio, objeto o bien jurídico protegido. Estos nuevos delitos informáticos (denominación ya acuñada en la práctica, pero falta de consagración jurisprudencial y legal) han sido positivados por primera vez por el legislador, pero todavía queda mucho camino por recorrer, dada la vertiginosa rapidez con que las TICS se expanden, evolucionan y desarrollan y con ellas las nuevas formas y figuras delictivas que comporta esta nueva realidad. (p.1)

> Artículo 197 bis.
>
> 1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el

> legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.
>
> 2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses. (Ley N° 1/2015)

El legislador español implementó dentro del ordenamiento jurídico el acceso no autorizado a un sistema informático, infringiendo el sistema de autenticación y de medidas de seguridad, pues es un hecho notorio que el ciberdelito se basa en el ingreso sin el consentimiento del titular, de esta manera se determina que en España contiene regulación sobre el Hacking.

En la reforma de 2015 introduce una serie de cambios, estableciendo que quien, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. Se debe destacar que se penará el simple acceso, aunque no se haya accedido a los datos. En cuanto a las medidas de seguridad, habrá que estar al adecuado estado

de la técnica, usos o costumbres. Como novedad se habla expresamente de colaboración, por el que se facilita a un tercero el acceso al conjunto o a una parte de un sistema de información. (Guardiola, 2016)

> Artículo 197 ter. Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:
>
> a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
>
> b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información. (Ley N° 1/2015)
>
> Artículo 197 quater.
>
> Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado. (Ley N° 1/2015)

Este tipo penal español tiene estricta relación al artículo 234 del Código Penal de Costa Rica, pues viene a tutelar la facilitación la consecución de un ciberdelito.

En Costa Rica implementa dentro del tipo penal otros verbos como la producción, la importación o adquisición.

En el artículo 197 quater del Código Penal de España, viene a regular un carácter de agravante cuando el delito informático es cometido por un sujeto perteneciente al crimen organizado, por esa razón hace necesario su pena mayor. Mas bien, se observa una gran diferencia en la tipificación, pues en el Código Penal de Costa Rica en el artículo 235 impone como agravante, cuando el ciberdelito afecte la lucha contra el narcotráfico o crimen organizado y no cuando el delito informático es cometido por algún delincuente del crimen organizado como lo tutela en el Código Penal Español.

> Artículo 278.
>
> 1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos. (Ley N° 1/2015)

Artículo 197 quinquies.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. (Ley N° 1/2015)

Se determina que la responsabilidad de las personas jurídicas de acuerdo al ordinal 197 quinquies del Código de España, se denota que existe una incerteza jurídica, pues pretenden sancionar con pena de multa las personas jurídicas, pero no indica cuál sería el parámetro económico correspondiente a la multa. En el Código Penal de Costa Rica, no hay ninguna norma penal que tenga estricta referencia sobre la responsabilidad de las personas jurídicas, ya que es un tema controversial. Algunos estudiosos indican que no es posible sancionar a una persona ficticia, pues vendría a establecer sanciones penales a los Representantes Legales de las Empresas, cuando los hechos delictivos, no fueron materializados por el representante judicial.

> Artículo 198.
>
> La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años. (Ley N° 1/2015)

Que de esta figura penal el legislador español impuso un supuesto de agravante a los servidores públicos, pues tienen una serie de facilidades para el acceso a la información para ejecutar un ciberdelito. En el Código Penal de Costa Rica, se logra determinar que ningún delito informático, tiene como agravante cuando el autor sea un funcionario público, es decir, que tenga una condición de agravante especial por la condición del servidor público. No obstante, lo que, si está regulado en Costa Rica, es cuando a causa del ciberdelito afecte servicios públicos, en ese caso, se estaría aplicando el agravante en los distintos tipos penales informáticos, los cuales permitan una pena mayor producto de ese hecho.

> Artículo 278.
>
> 1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado

> con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
>
> 2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
>
> 3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos. (Ley N° 1/2015)

El legislador español implemento dentro de su normativa el delito de Espionaje, y lo regula de una forma atinada, pues pretende proteger los datos corporativos o empresarial, que tienen un valor en el comercio muy fuerte, y por esa razón, hace que los ciberdelincuentes opten por delinquir de esta manera. En consecuencia, de ello el legislador español, impuso como conducta delictiva al que cede a terceros los secretos descubiertos. En el Código Penal de Costa Rica, a través del artículo 231, se regula el Espionaje Informático o Industrial tutelando también al sujeto que transmite, de allí la similitud con el Código Penal Español.

En relacion con este tipo penal ciertos autores indican que más bien, el Legislador Español, contempla el ilícito bajo carácter de peligro abstracto y no de resultado, pues contiene verbos de apoderarse, sin necesidad de una ulterior consecuencia producto de la conducta delictiva. (López & Torres, 2010)

No obstante, no se comparte dicho criterio, pues el tipo penal debe encausarse por ser un delito de peligro abstracto, ya que cuando el delincuente informático tenga en su poder la receta de la Coca Cola a modo de ejemplo, se le abre un sinfín de opciones en el mercado para su beneficio económico.

2.2.3 El Convenio de Budapest a la luz de la Legislación Sustantiva Costarricense.

Este Convenio de Budapest es un instrumento internacional que nació el 23 de noviembre del año 2001 en el Consejo de Europa, en donde tiene como fin luchar en contra del cibercrimen. Uno de los elementos prioritarios de este Tratado Internacional es que todos los países firmantes, se comprometen a tener una política penal común, ya que el fenómeno de las nuevas tecnologías (TICS), tiende a ser de carácter internacional.

Dentro del preámbulo de Convenio se enmarca el fenómeno de la nueva Era de la Tecnología, ya que contiene un riesgo enorme a causa de las redes informáticas, la información electrónica utilizada por los ciberdelincuentes para cometer los hechos delictivos dentro del ciberespacio. Dada esta circunstancia, es necesario prevenir de una forma efectiva, todos aquellos ciberdelitos dirigidos en contra de la confidencialidad, la integridad, la disponibilidad de los datos informáticos y sistemas informáticos, de los abusos de las redes y datos.

En otro orden de ideas, la Asamblea Legislativa de Costa Rica a través de la Ley N°4572 ratificó en todos sus sentidos el Convenio sobre la Ciberdelincuencia el día 03 de julio del año 2017, por ende, se adquirió una serie de compromisos a nivel internacional esto con el fin de cumplir con el objetivo del Convenio, que es la

creación de una Política Penal Común, así como su armonización a nivel internacional.

El Convenio de Budapest, brinda parámetros básicos que cualquier país que ratifico el Tratado, debe poseer dentro de su marco jurídico, y ello no impide que tenga más tipos penales que los exigidos por el Convenio de Budapest. (Chinchilla, 2015)

En cuanto a la estructura que contiene el Convenio en contra de la Delincuencia Informática, consta de 48 artículos. Dentro su redacción abarca cuatro capítulos, en donde el primero de ellos comprende los términos del argot informático, como segundo comprende la tipificación de los tipos penales, el capítulo tercero incluye el tema de la Cooperación Internacional, extradición, asistencia entre Estados, y el capítulo cuarto se refiere a las disposiciones finales del Tratado.

Obsérvese, en lo que respecta a los preceptos de aplicación material, se puede dividir, conceptualmente, en dos partes bien diferenciadas: Derecho Penal Internacional, constituido por las disposiciones 2 a 13, y Derecho Procesal Penal Internacional, en los artículos 14 a 35. Más adelante se prestará mayor atención al articulado y el mensaje que encierra el texto legal, baste anotar por ahora que la porción relacionada con el Derecho Procesal es cuantitativamente el doble que la sustantiva. (Gómez, 2010)

Por ende, se entrará a realizar el análisis a nivel sustantivo del Convenio de la Delincuencia Informática en relación con Código Penal de Costa Rica.

Medidas que deberán adoptarse a nivel nacional

Sección 1. Derecho penal sustantivo

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2. Acceso ilícito. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, el acceso deliberado e ilegítimo a la totalidad o una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático. (Ley N° 9452)

Este artículo del Convenio de Budapest pretende que los Estados firmantes implementen el hacking dentro de su ordenamiento jurídico. Debe entenderse el acceso ilícito como la intrusión a un sistema informático sin el consentimiento del titular, vulnerando las medidas de seguridad o las credenciales interpuestas al

dispositivo, pues con únicamente al ingresar ilegítimamente, se configuraría el delito. De esta manera, se observa que es no es delito de resultado, sino de peligro abstracto.

La prohibición penal en cuanto al acceso no autorizado puede brindar una protección adicional al sistema y a los datos propiamente dichos y en una primera etapa contra los peligros de suplantación de identidad. (Consejo de Europa, 2010)

Que de un estudio de la normativa penal costarricense se desprende que no se cuenta con el delito de acceso ilícito en el Código Penal. Es una conducta atípica, actualmente en donde quedan impunes todos aquellos ingresos ilegítimos de un sistema informático, violentando las medidas de seguridad impuestas a un ordenador.

La legislación costarricense, no cuenta con el tipo penal del Hacking, pues por cuestiones políticas se eliminó el borrador del Proyecto de Ley N° 9048. Los Diputados de la Administración de Laura Chinchilla, tenían el pensamiento que para el Hacking se configurara se requería de algún daño una vez que el delincuente informático realizara el ingreso ilegitimo y no consideraban pertinente tipificar únicamente el simple acceso ilegitimo. Que al final de cuentas, ese es el ADN de hacking. Por dicha razón se eliminó del borrador que se encontraba contemplado, pues se observó que no iba a existir voluntad política para la aprobación del Proyecto de Ley, y se decidió eliminarlo de la propuesta para que

los demás delitos informáticos, pasaran al Plenario Legislativo y fuese Ley de la República. (Chinchilla, 2015)

> **Artículo 3. Interceptación ilícita**. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, 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. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático. (Ley N° 9452)

Este tipo penal de Interceptación ilícita viene a tutelar la privacidad de las comunicaciones cibernéticas. De esta manera, debe entenderse la interceptación de medios técnicos cuando se refiere a vigilar, adquirir, el contenido de la información, ya sea de forma directa. Se da también por el acceso y el uso del dispositivo móvil con el fin de intervenir las comunicaciones privadas. Del tipo penal se extrae que la transmisión de datos informáticos no públicos tiene estricta relación con la naturaleza del proceso de transmisión, pues, nada impide que los datos sean accesibles al público, pero que los sujetos deseen manejarlo de forma

confidencial. No guarda relación alguna con el contenido de la información, si es pública o privada, sino que debe entenderse como el proceso de transmisión de los datos informáticos.

Que, de un análisis del marco jurídico costarricense, se desprende que este tipo penal, se encuentra cumplido por Costa Rica a través de los artículos 196 y 196 bis del Código Penal. Se fundamenta esta postura, ya que el artículo 196 del Código Penal de Costa Rica, protege la intimidad de las comunicaciones o correspondencia, en el sentido que es prohibido apoderarse, acceder, modificar, alterar, suprimir, intervenir, interceptar, abrir, entregar, vender, remitir, desviar, a su destino documentación o comunicaciones dirigidas a otra parte. Y más bien, el artículo 3 del Convenio de Budapest, solo se refiere a la interceptación deliberada e ilegítima a través de medios técnicos, datos informáticos provenientes de un sistema informático.

> **Artículo 4. Interferencia en los datos** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
>
> 2. Cualquier Estado Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado I provoquen daños graves. (Ley N° 9452)

Este tipo penal de Interferencia de Datos viene a proteger la integridad de los datos informáticos. De esta manera, debe entenderse el término como borrar como la eliminación total de un dato informático o un programa. Con relacion, al término de alterar se refiere a una conducta que supone una modificación con alcances negativos dirigido al dato informático, perdería su funcionalidad.

Que, de un análisis del marco jurídico costarricense, se desprende que este tipo penal, se encuentra cumplido por Costa Rica a través del artículo 299 bis del Código Penal. Se fundamenta esta postura, ya que el artículo 229 bis del Código Penal de Costa Rica, protege la integridad de la información, en el sentido que es prohibido suprimir, modificar, destruir la información contenida en un sistema informático, o una red informática, cuando no exista autorización del propietario de la información o si excede a borrar más de lo que le permitió el titular de la información. Inclusive se imponen agravantes cuando la información suprimida es irrecuperable. Y más bien, el artículo 4 del Convenio de Budapest, solo se refiere a la comisión deliberada de actos que afecten la integridad de los datos informáticos.

> **Artículo 5. Interferencia en el sistema.** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, 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. (Ley N° 9452)

Que este tipo penal de Ataques a la Interferencia en el sistema viene a proteger el funcionamiento correcto del sistema informático. Debe entenderse, el termino de obstaculizar como aquella acción que entorpece el debido funcionamiento a través de la introducción, transmisión, provocación de daños, borrado, alteración o supresión de datos informáticos.

Que, de un análisis del marco jurídico costarricense, se desprende que este tipo penal, se encuentra cumplido por Costa Rica a través del artículo 299 ter del Código Penal. Se fundamenta esta postura, ya que el artículo 229 ter del Código Penal de Costa Rica, protege el funcionamiento de un sistema informático, en el sentido que es prohibido destruir, alterar, entorpecer, impedir, alterar, obstaculizar o modificar sin autorización el funcionamiento de un sistema, de los componentes físicos o lógicos del sistema. Inclusive se imponen agravantes cuando el producto del sabotaje informático, cause algún daño colectivo, o si más bien el sistema informático pertenezca a la Administración Publica. Y más bien, el artículo 5 del Convenio de Budapest, solo se refiere a la obstaculización grave deliberada e ilegítima a través de las distintas vías de comisión de un delito informático.

> **Artículo 6. Abuso de los dispositivos.** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i. un dispositivo, incluido un programa informático adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; ----

ii una contraseña, un código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguno de los delitos previstos en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un determinado número de dichos elementos para que se considere que existe responsabilidad penal

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo, no tengan por objeto la

> comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático
>
> 3. Cualquier Parte podrá reservarse el derecho de no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, distribución o cualquier otras puesta a disposición de los elementos indicados en el apartado 1.a.ii del presente artículo. (Ley N° 9452)

De un estudio de la normativa penal de Costa Rica, se desprende que se cumple parcialmente con el parámetro del Convenio de Budapest, siendo que Costa Rica cuenta con el ordinal 234 que es referente a la facilitación de un delito informático, y supone que un sujeto le brinde los medios, herramientas a un delincuente para la ejecución de un ciberdelito. Así las cosas, únicamente se ajustaría al inciso a ii del articulo 6 titulado como Abuso de los Dispositivos. En relación con los demás supuestos, Costa Rica no contiene una norma penal expresa que tipifique la producción, venta, importación, difusión referente a la consecución de un delito informático.

> **Artículo 7. Falsificación informática.** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cuando se cometa de forma deliberada e ilegítima, 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 directamente legibles e inteligibles. Cualquier parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal. (Ley N° 9452)

De un estudio del bloque de legalidad penal de Costa Rica, se desprende que se cumple con lo exigido por el Convenio de Budapest, siendo que nuestro país cuenta con los artículos 366, 367, 368 del Código Penal referentes a la falsificación de documentos públicos, falsedad ideológica, y falsificación de documentos privados, todos ellos vienen a complementar lo requerido por el Convenio Internacional en contra de la ciberdelincuencia.

> **Artículo 8. Fraude informático.** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:
>
> a. cualquier introducción, alteración, borrado o supresión de datos informáticos;
>
> b. 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. (Ley N° 9452)

Del estudio de la normativa costarricense se desprende que según el artículo 217 bis del Código Penal de Costa Rica, supone a ajustarse con lo exigido en el Convenio de Lucha contra la Ciberdelincuencia, pues, este tipo penal es referente a la Estafa Informática que puede ser cometido a través de la manipulación, o si influye en el ingreso, procesamiento o resultado de datos de un sistema de información, así como el uso de indebido de datos falsos o incompletos. Por ende, se cumple a cabalidad con el Tratado Internacional.

> **Artículo 9. Delitos relacionados con la pornografía infantil.** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos:
> 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. 2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá 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 un menor comportándose de una forma sexualmente explícita

3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2. (Ley N° 9452)

De un estudio detallado de la normativa penal costarricense, se observa que se cuenta con tipos penales que se llegan a encuadrar en lo exigido por el Convenio de Budapest, siendo que, en Costa Rica, se tipifica la fabricación, producción o reproducción de pornografía, la tenencia de material pornográfico, la difusión de pornografía, y la pornografía virtual, de conformidad con los artículos 173, 173 bis, 174, 174 bis del Código de Penal de Costa Rica.

Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. 1. Cada Parte adoptará las medidas

legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, las infracciones de la propiedad intelectual, según se definen en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París del 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Propiedad Intelectual, a excepción de cualquier derecho moral otorgado por dichos convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, las infracciones de los derechos afines definidos por la legislación de dicha Parte, de conformidad con las obligaciones que ésta haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático

> 3. En circunstancias bien delimitadas, cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo. (Ley N° 9452)

Del bloque de legalidad costarricense se desprende que se cuenta con los tipos penales requeridos por el Convenio de Budapest, en el sentido que a través de los artículos 44, 45, 46, 47, 48, 51, 52, 53, 54, 55, de la Ley N° 8039 de Procedimientos de Observancia de los Derechos de Propiedad Intelectual se regula todo lo referente con los derechos de autor y conexos. En ese sentido, se cumpliría con el artículo de la Ley Especial en relación con el Tratado Internacional.

> **Artículo 11. Tentativa y complicidad.** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previsto de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, cualquier tentativa de comisión de alguno de los delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a y c. del presente Convenio, cuando dicha tentativa sea intencionada

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo. (Ley N° 9452)

En relación con este artículo del Convenio de Budapest, se desprende que Costa Rica desde vieja data mantiene tutelado el tema de la tentativa y la complicidad a través de los artículos 24 y 47 del Código Penal de Costa Rica.

Artículo 12. Responsabilidad de las personas jurídicas. 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas, por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a. un poder de representación de la persona jurídica;

b. una autorización para tomar decisiones en nombre de la persona jurídica;

c. una autorización para ejercer funciones de control en la persona jurídica

2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad

3. Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de la persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito. (Ley N° 9452)

Sobre este artículo del Convenio de Budapest, pretende que las personas jurídicas sean sujetos de reproche penal cuando sean autores de un delito informático, pues en Costa Rica, no existe una norma penal que sancione a las personas jurídicas ni tampoco es viable la tutela, pues desconocería los principios básicos del Derecho Penal, siendo que la pena más gravosa como la privativa de libertad debe ser interpuesta a una persona física, no a una ficticia. En síntesis, es un tema controversial por los alcances que tendría y las distintas posiciones jurídicas existentes en el medio.

2.2.3.1 El Hacking y sus formas de ensayo a nivel Internacional

El acceso ilícito a un sistema informático es una conducta delictiva que viene acompañada desde los inicios de la ciberdelincuencia. Este fenómeno del hacking se refiere al acceso no autorizado a un sistema informático, de esta forma los bienes jurídicos afectados serían la intimidad cibernética de cada titular y la seguridad informática impuesta al sistema informático o a un dispositivo móvil.

Esta clase de delito debe considerarse siempre como un delito de peligro abstracto y no de resultado, pues, el bien jurídico tutelado es la intimidad y la ciberseguridad violentada. No es necesario que aparte del ingreso ilegitimo realice un acto delictivo dañoso, por ejemplo, no requerirá que acceda ilegítimamente al sistema y suplante la identidad del titular en redes sociales.

En otro orden de ideas, desde la óptica informática, existen dos clases de hackers en el ciberespacio: están los sombreros blancos y los negros. Los primeros incurren en la detección de vulnerabilidades de un sistema informático,

esto con el fin que el desarrollador o titular del sistema realice las mejoras pertinentes, es decir, vela para que no exista ninguna brecha de información dentro de las operaciones mercantiles. En cambio, los hackers sombreros negros, son aquellos especialistas en la informática, quienes aprovechan su conocimiento para acceder ilegalmente a un sistema informático, sacando provecho de las vulnerabilidades del sistema y de esa forma extorsionar al titular de la información por la no destrucción de archivos que contienen un valor comercial importante. Este tipo de hacker accede a un sistema informático con un fin de dañar.

Ahora bien, desde el plano internacional ciertos países han decidido tipificar este ciberdelito dentro de su marco jurídico. Dicho esto, cada uno de los países en función de la soberanía de cada Estado decidieron tutelarlo a través de distintas maneras. Esto con el fin de evitar que Costa Rica cuente con falencias el bloque de legalidad referente a la ciberdelincuencia de nuestro país.

El art. 615 ter del Código Penal Italiano dispone: El que abusivamente se introduce en un sistema informático o telemático protegido por medidas de seguridad o bien se mantiene en él contra la voluntad expresa o tácita de quien tiene derecho a excluirlo, es penado con pena de prisión de hasta tres años. (Ley N°63)

Se observa que en el marco jurídico italiano con relacion al hacking, se denota que cumple con los requerimientos indicados por el Convenio de Budapest en el

sentido que posee dentro de su terminología la violación de una medida de seguridad, pues es un hecho implícito del dispositivo o el computador.

Según esta regulación del intrusismo informático, la legislación italiana no requiere adaptación alguna al proceso de armonización que en esta materia realiza la Decisión-marco, pues sobradamente se respetan las exigencias de esta al superarse sus requisitos mínimos. (Matellanes, 2008)

El artículo 269 A del Código Penal de Colombia indica: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho a noventa y seis meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. (Ley N°1273)

Que, según la regulación de Colombia, se desprende que el intrusismo informático se configura cuando el ciberdelincuente violenta las medidas de seguridad impuestas al sistema informático y por ende no existe no existe un consentimiento del titular. Como un hecho notorio, aparte de la sanción privativa de libertad a imponer, también incluyen una pena de multa por los daños ocasionados.

El artículo 197 bis.1 del Código Penal de España dispone: El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. 2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses. (Ley N° 1/2015)

Que, del Código Penal de España, se desprende que tipifican no solo el acceso ilegitimo sino también a la persona que facilita, es decir, que le brinda los medios o información para que se dé el intrusismo informático dentro del sistema. Por ende, el ciberdelincuente accesa al sistema de una forma no consentida por el titular.

Ningún país que se citó dentro de su marco jurídico contempla dentro del tipo penal si el hacker ingresa al sistema informático con un fin malicioso o no, ya que los hackers per se no son delincuentes informáticos, sino que dependerá del uso dado al conocimiento cibernético.

2.2.4 Judicialización de los ciberdelitos y la obtención de la prueba en el exterior.

2.2.4.1 El cibercrimen como conocimiento y su aplicación práctica.

Dado este fenómeno de las nuevas tecnologías (TICS) y las nuevas conductas delictivas que aparecen día a día en la convivencia, es necesario que dichos hechos delictivos se lleven a la sede jurisdiccional, esto con el fin que un Juez de la República determine la culpabilidad o la inocencia del ciberdelincuente. Ante este fenómeno delictivo realizado en el ciberespacio, es necesario que los jueces cuenten con un conocimiento técnico, pues, la materia informática requiere de ello.

Ahora bien, en el circulante de los Tribunales Penales hubo un caso en donde se tuvo como acreditados estos hechos: El día 4 de enero del año 2013 la imputada GBH con conocimiento de la clave de acceso o PIN de la cuenta 001-0169783-8 del Banco de Costa Rica perteneciente al ofendido, la imputada GBH

influyó en el sistema desde el número de teléfono 2255-59-88 y sin autorización alguna transfirió a su cuenta bancaria número 001-0214621-5 del Banco de Costa Rica la suma de 500.000 colones, dinero que retiró la imputada GBH de un cajero automático. 2.-El día 8 de enero del año 2013 la imputada con conocimiento de la clave de acceso de la cuenta 001-0169783-8 del Banco de Costa Rica perteneciente al ofendido, la imputada influyó en el sistema desde el número de teléfono 7076-05-58 y sin autorización alguna transfirió a su cuenta bancaria la suma de 30.000 colones, dinero que retiró la imputada de un cajero automático. 3- El día 7 de enero del año 2013 la imputada con conocimiento de la clave de acceso de la cuenta 001-0170623-3 del Banco de Costa Rica perteneciente al ofendido, la imputada influyó en el sistema desde el número de teléfono 2263-69-30 sin autorización alguna transfirió a su cuenta bancaria la suma de 200.000 colones, dinero que retiró la imputada GBH de un cajero automático. 4- Una vez acreditados los montos en la cuenta de destino, se registraron varios movimientos por medio de los cuales se retiró el dinero. (Voto N° 2016-0450, Tribunal de Apelación de Sentencia Penal)

El Tribunal Penal tuvo como acreditada la conducta de Hurto Agravado, pues, aseveran que la imputada no manipulo los datos y no influyo en su procesamiento ya que ingreso la clave que hubiese puesto el titular de la cuenta. De esta manera, el fundamento del Tribunal de primera instancia es errónea, ya que se debió haber aplicado la Estafa Informática por el uso indebido de datos, por esta razón el Tribunal de Apelación recalifico los hechos a este ciberdelito. El fundamento del juzgado de primera instancia para tener por acreditado el hurto agravado es sin

lugar, pues, antes de la entrada en vigor de la Ley N° 9048 se aplicaba de esa manera a través del hurto agravado, y no el fraude informático, pues antes de la entrada en vigencia de dicha ley, existía un vacío en la ley que le abría un portillo a los ciberdelincuentes desplegar la conducta delictiva sin ninguna sanción penal, por ello a nivel del Poder Judicial se decidió aplicar la figura del hurto agravado. Nótese que la sentencia del Tribunal Penal es del 2015, es decir cuando ya la reforma estaba en vigencia, esto significa que existió en este caso un desconocimiento de la reforma a la legislación de los delitos informáticos implementada en nuestro marco jurídico, por ende, se incurrió en una mala aplicación sustantiva del tipo penal.

En relación con un factor importante para la aplicación práctica de los delitos informáticos son las capacitaciones a nivel nacional o internacional, para los operadores del derecho, en donde anteriormente las invitaciones a los cursos solo le enviaban al Ministerio Público y un personero del OIJ, es decir, no contemplaban a la Judicatura. Se podía notar en los distintos cursos que tuvo participación algún Juez de la República que era el primer contacto internacional referente a los delitos informáticos y todas las consultas se basaban en aspectos muy básicos. Por ello es necesario que todos estén en la misma sintonía. (Segura, 2018)

Ahora bien, en un caso real en donde la novia solicita ante una telefonía una línea a nombre de ella, y se la regala al novio para que se pueda comunicar con ella, posteriormente la novia sospecha que le está siendo infiel y procede con la revisión del celular, los chats de WhatsApp. Además, recibe y envía mensajes en

Tabla No. 1
Detalle de casos según Delito por Provincia.

nombre del usuario que es el novio. Sucede que el novio se apersona al Ministerio Público para presentar la denuncia y dicha entidad acusadora califican este delito como Estafa Informática. Es claro, que se está frente de un delito de suplantación de identidad y otros ciberdelitos. (Medrano, 2018)

De esta manera, todos estos factores al final de cuentas tienen una repercusión en la cantidad de condenatorias que emiten los Tribunales de Justicia referentes a los ciberdelitos. Este nuevo fenómeno de las nuevas tecnologías (TICS) debe entenderse como un compromiso para cualquier operador del derecho, pues exige su debido estudio al ser una rama del Derecho tan técnica, y en su apogeo.

	Provincia							
	San José	**Alajuela**	**Heredia**	**Cartago**	**Limón**	**Puntarenas**	**Guanacaste**	**Total General**
Suplantación de identidad	414	122	87	171	71	64	28	957
Estafa informática	174	131	122	69	86	49	78	709
Suplantación de páginas electrónicas	184	43	27	12	7	10	2	285
Difusión de información falsa	155	9	13	7	7	8	6	205
Seducción o encuentro con menores por medios electrónicos	113	13	22	20	3	8	0	179
Facilitación de delito información	10	1	39	5	42	12	1	110
Espionaje informático	64	4	2	2	1	0	0	73
Sabotaje informático	39	9	3	0	2	3	10	66
Violación de correspondencia	9	14	8	1	2	10	6	50
Daño informático	25	2	4	1	2	3	4	41
Instalación o propagación de programas informáticos maliciosos	3	0	1	1	1	0	0	6
Sustracción, desvió o supresión de correspondencia	2	0	0	0	0	1	0	3
Captación indebida de manifestaciones verbales	1	0	0	1	0	0	0	2
Total general	**1193**	**348**	**328**	**290**	**224**	**168**	**135**	**2 686**

Fuente: Datos tomados del Sistema IPH, Oficina Planes y Operaciones del Organismo de Investigacion Judicial (agosto 2015-2018)

De esta manera, se observa que San José es el lugar donde se presentan con mayor ocurrencia denuncias por el delito de suplantación de identidad, seguido de la Estafa Informática.

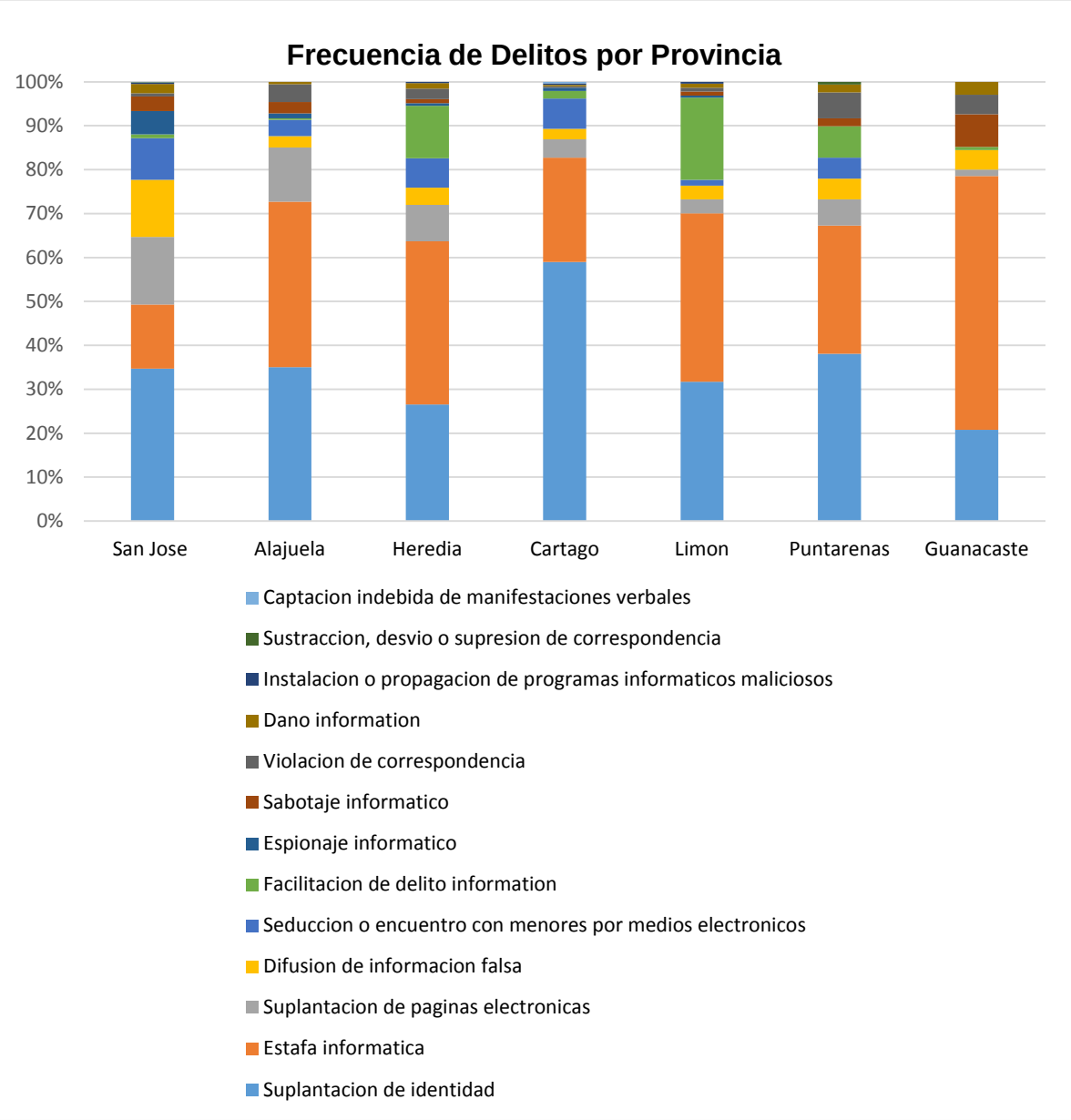


Figura 1

Frecuencia de delitos por Provincia

Fuente: Datos tomados del Sistema IPH, Oficina Planes y Operaciones del Organismo de Investigacion Judicial (agosto 2018)

Se observa con mayor claridad que la gran comisión de hechos delictivos por parte de los delincuentes informáticos, se dan a su vez suplantando la identidad virtual del usuario dentro de las plataformas tecnológicas de las grandes empresas como Facebook, Google, Yahoo y otras.

2.2.4.2 La Evidencia Digital

La evidencia electrónica debe definirse como un conjunto de metadatos almacenados, creados o transmitidos contenidos en un dispositivo móvil, o un sistema informático que servirá dentro del litigio penal, como un mecanismo de defensa o más bien como un elemento probatorio para fundar la demostración de culpabilidad. Debido a que el Internet no posee fronteras todos los elementos probatorios normalmente están alojados en el exterior, por ello se acude a la cooperación internacional para la obtención de la prueba en el exterior.

Por la multidimensionalidad territorial de la evidencia digital, nace la necesidad de gestionar los trámites para la obtención prueba electrónica en el exterior ante las empresas norteamericanas como lo son Microsoft, Google, Apple, Facebook, WhatsApp, ya que son contenedoras de una gran cantidad de datos de contenido correspondientes a usuarios registrados a nivel mundial, pues esa información serviría enormemente para la investigación de un delito informático, ya que estas plataformas tecnológicas son utilizadas como medio para la comisión del ciberdelito.

Ahora bien, con respecto a la solicitud de obtencion de prueba al exterior dirigido a las grandes empresas, se puede determinar que ellas actúan bajo principios de buena fe únicamente, no hay forma de imponer medidas coercitivas ante la no respuesta oportuna. Dichas empresas domiciliadas en Estados Unidos solo brindan evidencia digital cuando Facebook a modo de ejemplo considere que debe

darse la respuesta al requerimiento legal, pues puede existir un peligro para el usuario o también cuando consideren pertinente evitar o identificar hechos de fraudes, usos no autorizados de productos de la compañía, o alguna violación a las políticas de privacidad de la empresa. Todo esto se debe, ya que los Estados que solicitan la evidencia digital, provienen de una jurisdicción ajena a la de los Estados Unidos.

Existe un gran problema específicamente en Facebook, ya que, si se cuenta con la suerte que contesten la solicitud de asistencia internacional para la obtención de la prueba digital alojada en el exterior, dan respuesta al requerimiento, cuando la causa penal está a punto a prescribir o en caso contrario ni siquiera contestan el requerimiento. Como otro punto, si se envía la solicitud de asistencia internacional a través de una vía informal, es decir, por medio de un contacto, ni siquiera contestan, por ello se torna en compleja la investigación para la recolección de la prueba, cuando se dependa de empresas extranjeras. (Segura, 2018)

Es una dificultad para la investigación de un delito informático, la carencia de una cooperación internacional por parte de las grandes empresas, ya que dificulta el curso del proceso penal, en el sentido que se depende de la información electrónica alojada en el exterior para demostrarle al Tribunal la culpabilidad del delincuente. Así las cosas, dependiendo del caso en concreto provocaría que el Ministerio Público solicite el sobreseimiento definitivo de la causa por no tener elementos probatorios suficientes para imputar al delincuente informático.

Ahora bien, con respecto a delitos contra el honor como la difamación, injurias, calumnias tipificados en el código Penal de Costa Rica y que pueden ser cometidos a través de las plataformas tecnológicas como Facebook, Twitter, Instagram. Resulta que al no estar tutelados como delitos las acciones en contra del honor, en los Estados Unidos de América, sino que se considera como una infracción civil, dichas grandes empresas no brindan la información de datos de tráfico, pues se requiere la doble incriminación.

De esta manera, lo importante sería que nazca una plataforma de diálogo con las empresas domiciliadas en el exterior como Facebook, Yahoo, Apple, Google, Microsoft, esto con el fin de facilitar la cooperación internacional a través de la adición de una cláusula en las políticas de privacidad de las empresas extranjeras o nacionales, si cuentan con el permiso del usuario de la cuenta para que faciliten la información de una forma ágil en el marco de una investigación criminal, lo tendrán que realizar. Por ello a través de la Comisión Nacional de Lucha contra la ciberdelincuencia se establecerán protocolos de actuación para este tipo de cooperación, esto inclusive permitiría la creación de una plataforma tecnológica como lo tiene Apple, en donde a través de la firma digital del investigador permitiría que soliciten la prueba del exterior a las grandes empresas, ello incluiría un registro del investigador que solicitó la información, dando solidez a la trazabilidad, de conformidad con la propuesta de Proyecto de Ley N° 21187. (Medrano, 2018).

Por ende, se analizará de acuerdo con los datos estadísticos como los casos reportados, denuncias, la cantidad de resoluciones condenatorias y absolutorias registradas en el Poder Judicial para determinar porcentualmente la efectividad del proceso penal ante la investigacion de los delitos informáticos en Costa Rica.

Tabla No. 2

Casos denunciados por Delitos Informáticos, según provincia por año.

Periodo: 01 de enero del 2015 al 07 de agosto del 2018

	Año				
Provincia	2015	2016	2017	2018	Total General
San José	251	290	409	243	1193
Alajuela	54	80	118	96	348
Heredia	70	77	124	57	328
Cartago	44	77	102	67	290
Limón	21	42	78	83	224
Puntarenas	24	38	68	38	168
Guanacaste	28	32	38	37	135
Total	**492**	**636**	**937**	**621**	**686**

Fuente: Datos tomados del Sistema IPH, Oficina Planes y Operaciones del Organismo de Investigacion Judicial (agosto 2015-2018)

De esta manera se desprende que la provincia en donde existe una mayor comisión de delitos informáticos es en San José, luego le sigue Alajuela, y Heredia, y tiene sentido, pues en dichas provincias es donde existe una mayor

fuerza laboral y mayor uso de las tecnologías en razón de un ámbito laboral, profesional o académico de cada sujeto.

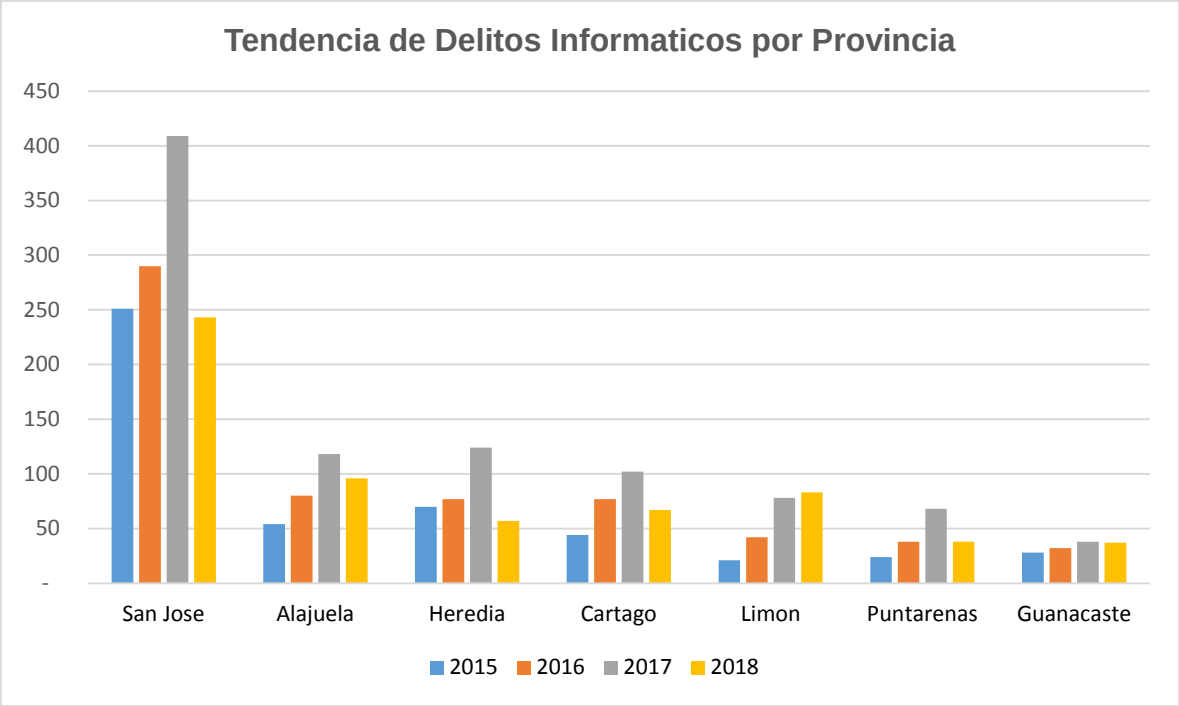


Figura 2

Tendencias de ocurrencia de delitos informáticos

Fuente: Datos tomados del Sistema IPH, Oficina Planes y Operaciones del Organismo de Investigacion Judicial (agosto 2015-2018)

Con este gráfico se pueden observar las tendencias a nivel de comisión de delitos informáticos durante el año 2015 al 2018 en las distintas provincias del país, en donde la capital es la puntera como el lugar con mayor ocurrencia producto de los ciberdelitos.

Ahora bien, dentro de la administración de justicia se cuenta con el dato numérico de las Sentencias absolutorias y condenatorias dictadas los Tribunales Penales, juzgando causas penales de delitos informáticos.

Tabla 3

Personas Condenadas y Absueltas por Tribunales Penales

Delito y Titulo del Código Penal	Condenatorias	Absolutorias
CONTRA EL HONOR		
Calumnias	9	52
Difamación	14	53
Injurias	27	160
SEXUALES		
Difusión de Pornografía	14	14
Fabricación, producción o reproducción de pornografía	2	1
Seducción o Encuentros con menores por medios electrónicos	4	0
Seducción o Encuentros con menores de edad	2	0
Tenencia de material pornográfico	2	1

CONTRA EL AMBITO DE LA INTIMIDAD Violación de Comunicaciones Electrónicas (Artículo 196 Bis)	4	0
CONTRA LA PROPIEDAD Fraude Informático	51	48
Estafa Informática	1	5
Total	**132**	**334**

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. (diciembre 2015-2017)

De esta forma, se observa claramente que más del 50% de los procesos penales durante el periodo 2015 al 2017, específicamente de los delitos informáticos que se tramitan en la vía judicial se llegan a absolver.

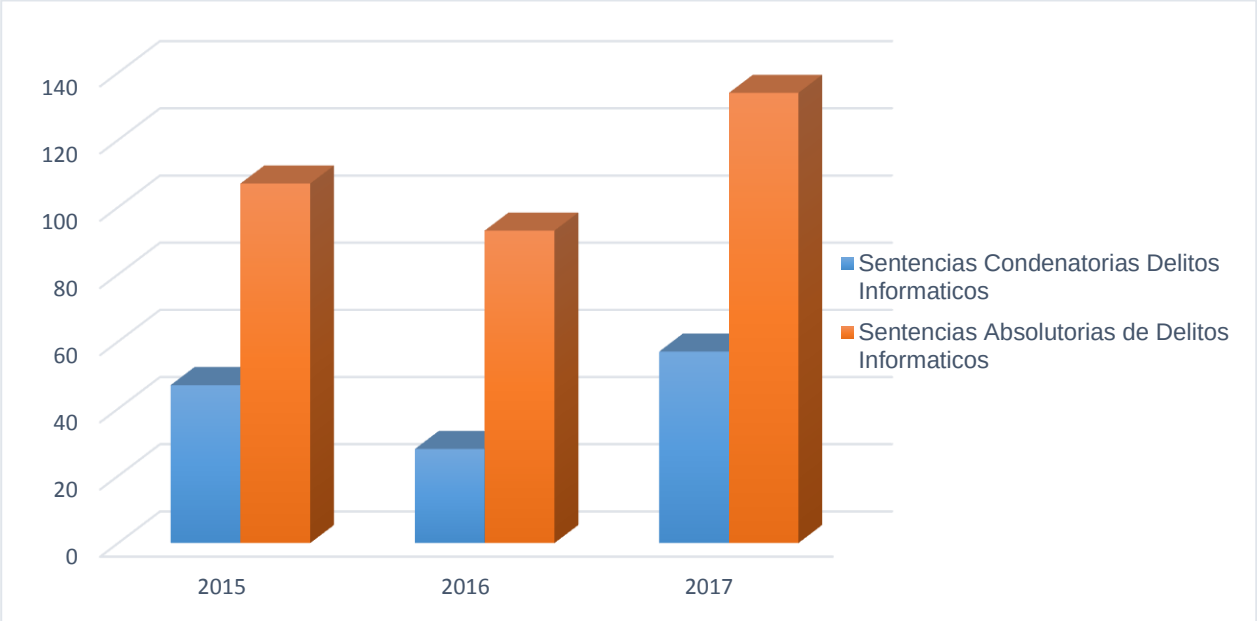


Figura 3

Cantidad de Sentencias Condenatorias y Absolutorias en un Proceso Penal de Delitos Informáticos

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. (diciembre 2015-2017)

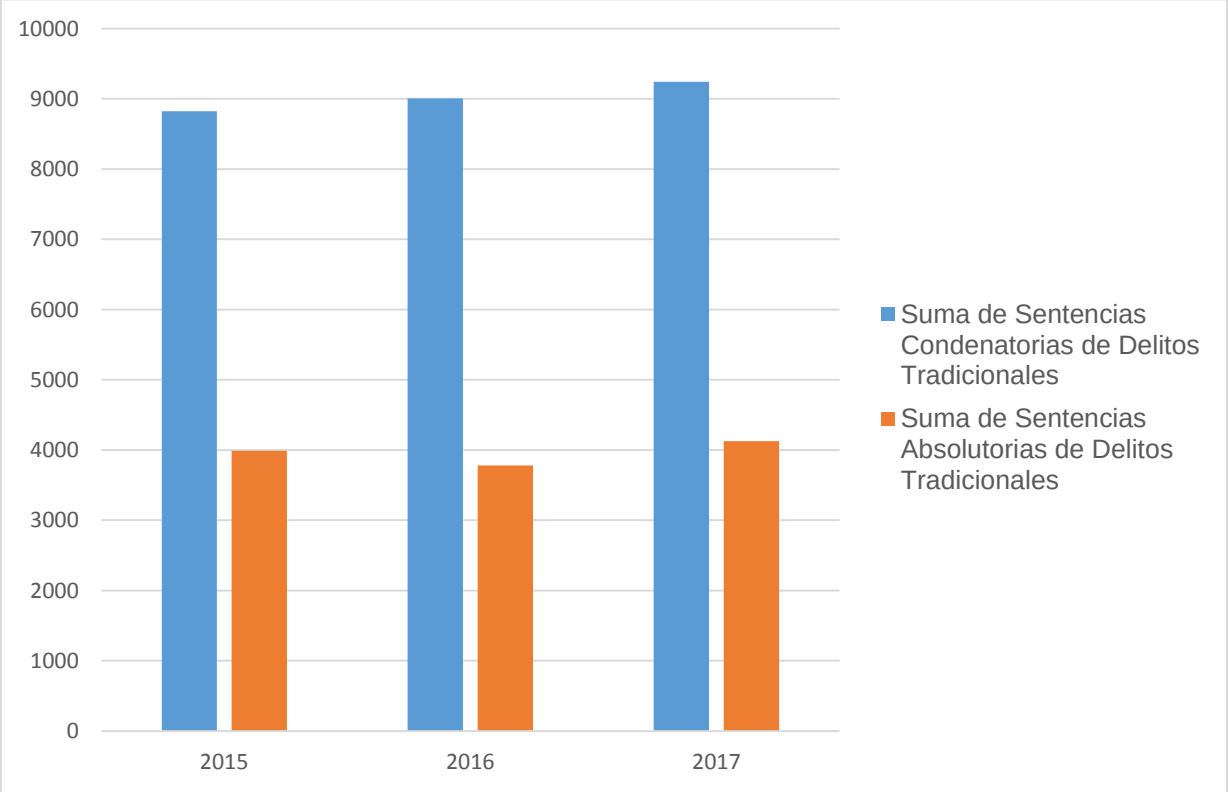


Figura 4

Cantidad de Sentencias Condenatorias y Absolutorias en un Proceso Penal de Delitos Tradicionales

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. (diciembre 2015-2017)

Ahora bien, realizando una comparación de los gráficos que tienen una Sentencia judicial a nivel de los delitos informáticos y los tradicionales se puede determinar, que en el caso de los ciberdelitos cuentan con un mayor grado de absolutorias, siendo necesario la obtencion de evidencia digital para demostrar la

culpabilidad y al no contar con dicho elemento el Tribunal de Juicio puede no tener una certeza cierta de la culpabilidad del delincuente informático, por ello el Tribunal no se puede decantar por la condena. En el caso de los delitos tradicionales es diferente, ya que la comisión de los mismos es llevada a cabo en la vida material o física, por ello las pruebas son naturalmente distintas. Contrario a lo sucedido con los delitos informáticos que tienen lugar en el ciberespacio.

En este expediente penal número 10-000013-0016-PE el Tribunal Penal del II Circuito Judicial de Alajuela llegó a absolver al imputado, ya que la empresa Google Inc no atendió la solicitud de asistencia internacional de Costa Rica durante la investigacion de un delito de Difamación, siendo que se requería la Dirección Ip y las bitácoras de acceso. Mediante un Oficio 354-SDI-201 de la Sección de Delitos Informáticos indicó que: Finalmente, la única forma de obtener las direcciones utilizadas para accesar dicho correo, es que su autoridad realice los trámites legales correspondientes, para que una autoridad en Estados Unidos le solicite a la empresa Google.com dichas bitácoras de acceso, indicando la dirección IP, la fecha y hora de cada acceso. Sin embargo, no hubo respuesta por parte de dicha empresa.

Luego en el expediente judicial número 13-000058-0621-PE el Juzgado Penal de la Función Pública, llego a desestimar la causa penal por insuficiencia probatoria en el sentido que no habían elementos objetivos que determinaran con claridad la información y además que no es posible identificar a ciencia cierta si una cuenta de correo Gmail fue vulnerada, ya que según la experiencia forense se

ha logrado determinar cómo dichas cuentas son administradas desde los Estados Unidos y solo tienen un backup de Direcciones Ip únicamente de treinta días. Incluyendo la dificultad de obtencion de dicha evidencia digital ante dichas empresas.

Posteriormente en el expediente judicial 10-000031-361-PE, se llegó a absolver por el principio universal In dubio Pro Reo, ya que el querellante no solicito ante los estrados judiciales un auxilio judicial previo para verificar si el correo electrónico difamatorio pertenecía a la dirección IP de la querellada, por ello indica el Tribunal de este modo, el que no se aportara copia certificada del correo electrónico; no se trajera al proceso al otro destinatario de esa comunicación; ni se buscara información tendiente a determinar que el peso del mensaje o número de caracteres fuera el mismo desde el envío de la dirección IP de la acusada al correo del señor y de este al correo de la querellante.

Y si hubiesen solicitado información a la empresa Yahoo tampoco hubieran respondido, es decir, el resultado en el proceso penal seguiría siendo el mismo, esto a criterio del suscrito, ya que es una tónica en las investigaciones de los delitos informáticos en Costa Rica.

Además, debe entenderse la Tutela Judicial Efectiva para los siguientes gráficos como el derecho que poseen las personas de acudir al sistema judicial para que un juzgador a través de una resolución debidamente fundamentada acoja o declare sin lugar la pretensión dada por una parte u otra, o en su caso declarar la

culpabilidad o inocencia del endilgado durante el desarrollo del proceso penal. De esta manera habilita a que cualquier ciudadano tenga acceso a la justicia y por otro lado permite la protección de los derechos fundamentales y de los bienes jurídicos penalmente relevantes dentro de la legislación.

En relación con la información de la cantidad de soluciones alternas aplicadas en los ciberdelitos existe una limitante en el sentido que el Poder Judicial no facilita dichos datos tan específicos ni se encuentran detallados por el tipo de delito requerido, sino que lo manejan a nivel macro, por ello en estos gráficos se correlaciona la tutela judicial efectiva en relación con las denuncias y las sentencias en los periodos.

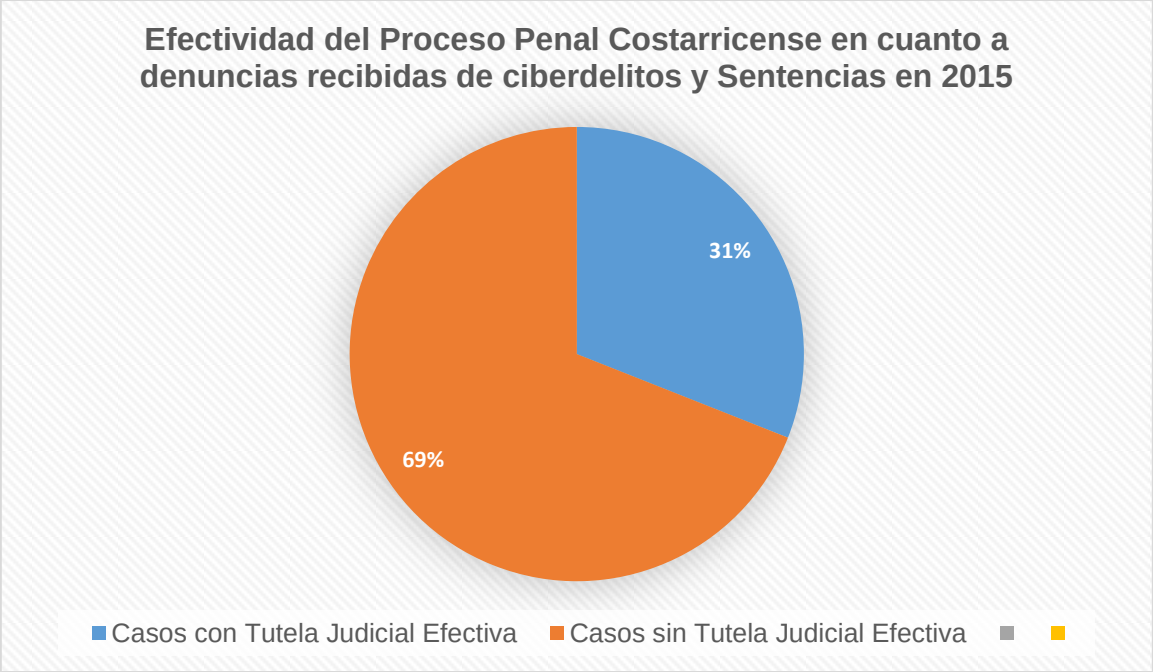


Figura 4

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias de ciberdelitos y sentencias en 2015

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. *(*diciembre 2015-2017)

Queda claro que, en el año 2015, únicamente alcanzó un rango de 31% en relación con la tutela judicial efectiva.

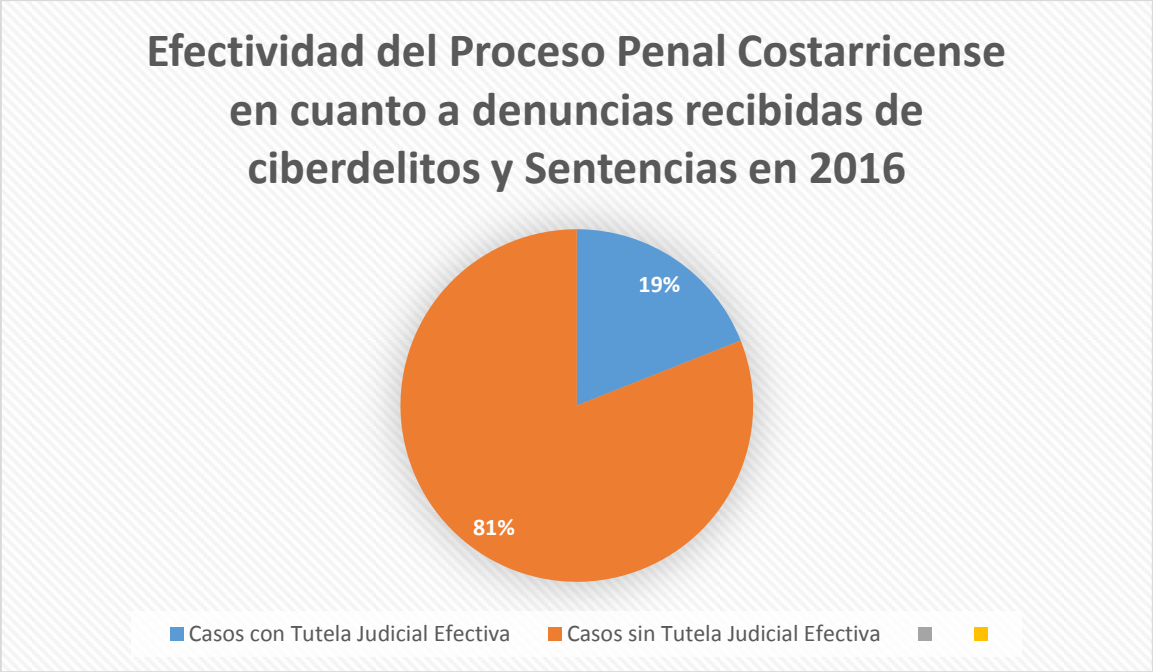


Figura 5

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias de ciberdelitos y sentencias en 2016

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. *(*diciembre 2015-2017)

Se mantiene el grado porcentual en el 2016 con niveles demasiado bajos y que de alguna manera repercuten en la salvaguarda de derechos fundamentales de los ciudadanos.

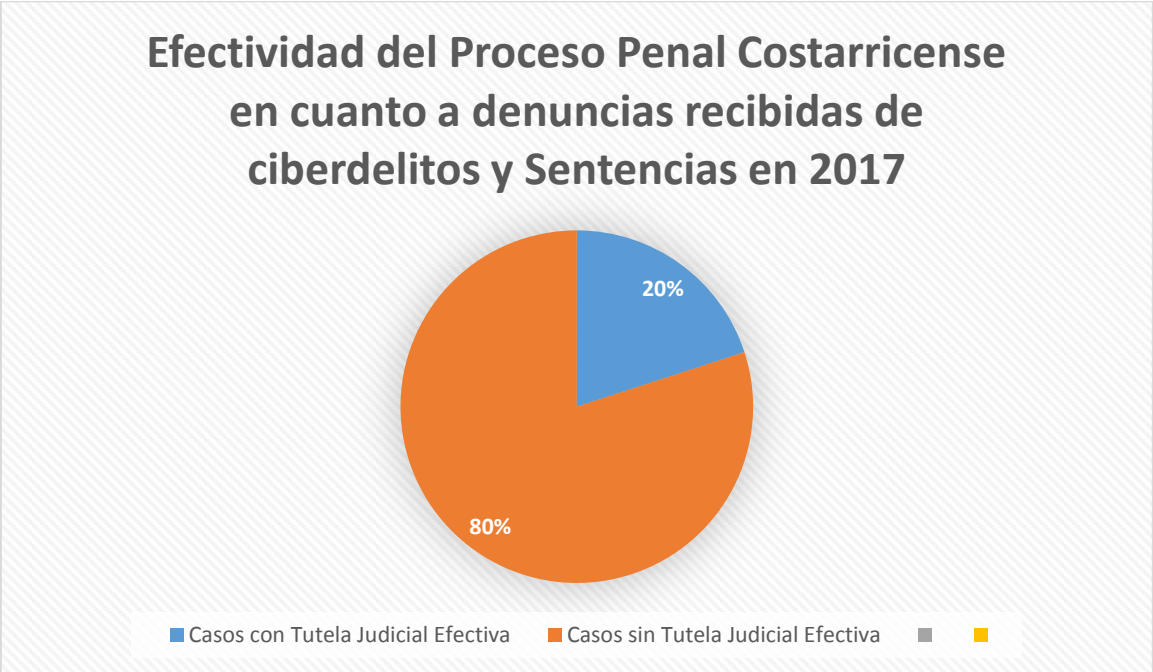


Figura 6

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias de ciberdelitos y sentencias en 2016

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. *(*diciembre 2015-2017)

Analizando lo anterior, se desprende que el grado porcentual de efectividad del proceso penal costarricense ante un delito informático mantiene indicadores muy bajos. Es decir, el sistema judicial no le brinda al ciudadano una tutela judicial efectiva en la investigacion del delito informático, pues la obtención de evidencia digital del exterior es medular para identificar la autoría del delincuente informático, así como la generalización de los domicilios de las grandes empresas que citan en los Estados Unidos.

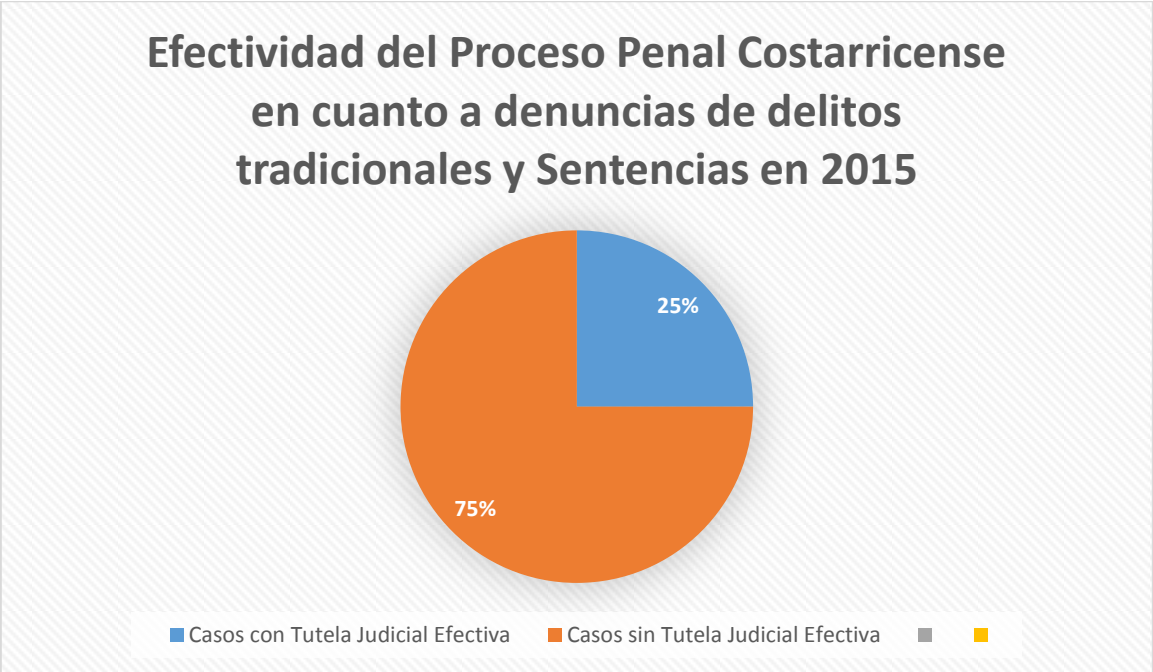


Figura 7

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias tradicionales y sentencias en 2015

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. *(*diciembre 2015-2017)

En estos casos correspondientes de delitos tradicionales, se determina que solo el 25% de los mismos obtuvieron una decisión judicial emitida por los Tribunales de Justicia. Debe considerar que la cantidad de denuncias convencionales aumenta en función de la tipificación establecida en el Código Penal.

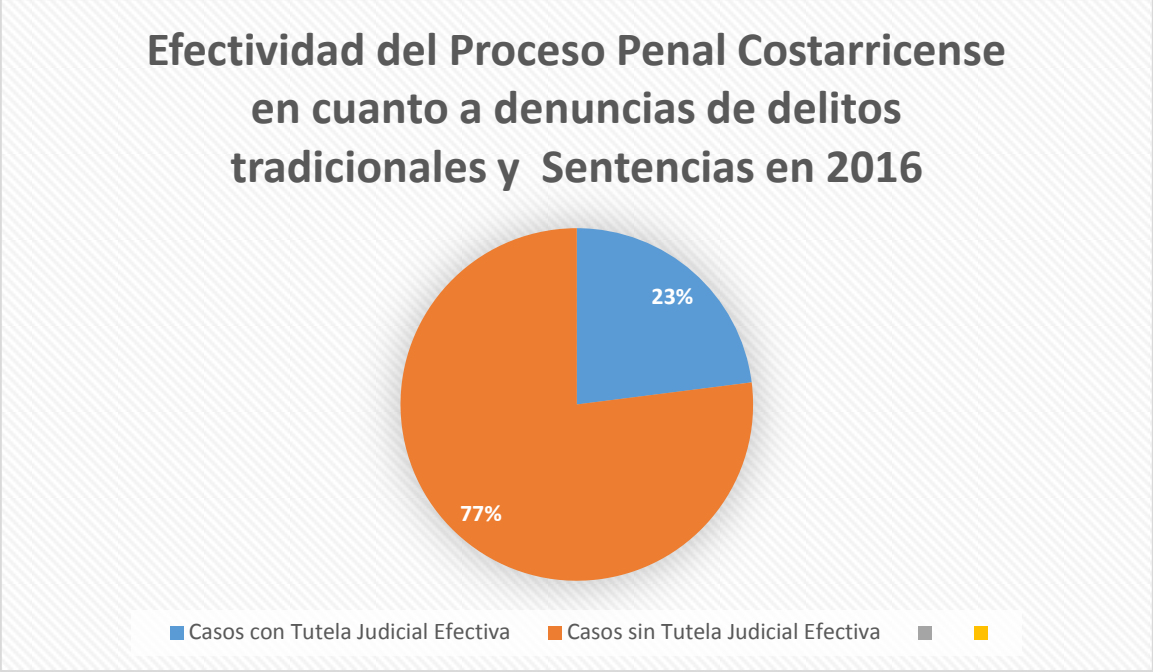


Figura 8

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias tradicionales y sentencias en 2016

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. (diciembre 2015-2017)

Ahora bien, se determina que la tutela judicial correspondiente a los delitos tradicionales fue de un 23%, mientras en comparación con el año 2016 correspondiente a los ciberdelitos es de un 19%. Existió un aumento en la cantidad de resoluciones judiciales emitidas referentes a tipos penales convencionales.

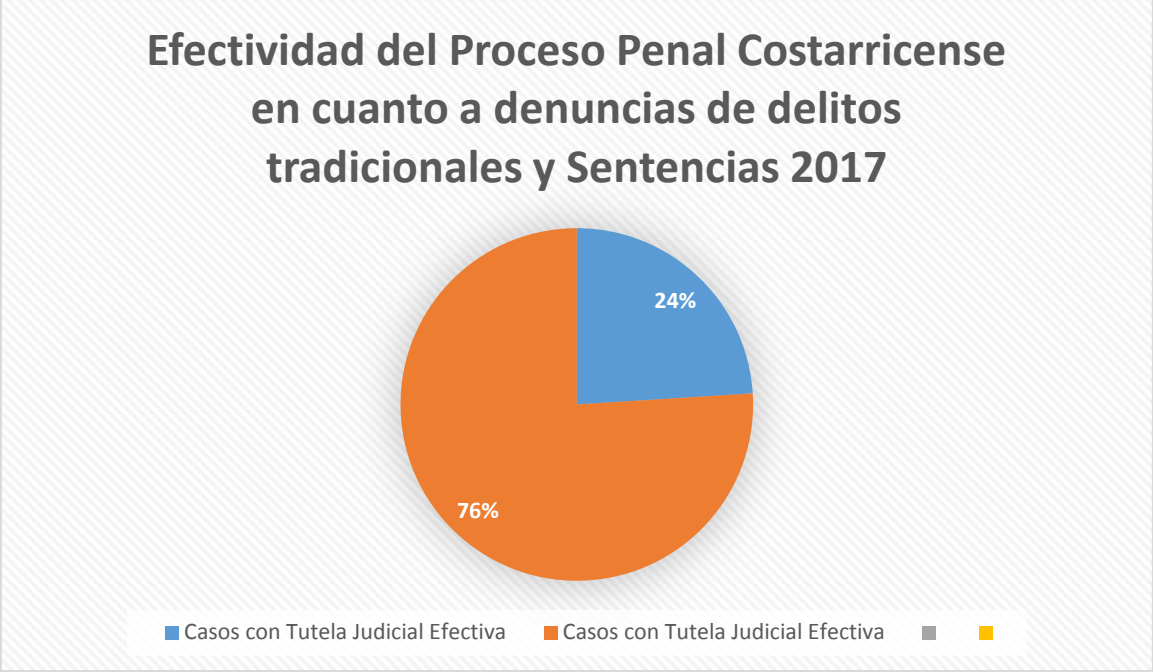


Figura 9

Efectividad Porcentual del proceso penal costarricense en cuanto a denuncias tradicionales y sentencias en 2017

Fuente: Datos tomados de Subproceso de Estadística, Dirección de Planificación del Poder Judicial. (diciembre 2015-2017)

De esta forma, se determina que la tutela judicial correspondiente a los delitos tradicionales fue de un 24%, mientras que el año 2017 correspondiente a los ciberdelitos fue de 20%. Se comprueba a todas luces que la tutela judicial brindada a los tipos penales tradicionales es mucho mayor a los ciberdelitos y sin contar que la cantidad de tipos penales convencionales es considerablemente mayor que los ciberdelitos.

2.2.4.3 Fundamento Jurídico Nacional para la obtención de la Prueba

En virtud que la prueba puede estar en territorio nacional o internacional la recolección de estas se fundamentan en normas nacionales y en Tratados internacionales esto con el fin de garantizar una tutela judicial efectiva.

La obtención de la prueba en el exterior en sede penal se encuentra fundamentada en los artículos 39 y 41 de la Constitución Política De Costa Rica. En donde nuestra carta magna garantiza el debido proceso en el sentido que para que un ciudadano busque justicia en los Tribunales debe necesariamente demostrarse a través de la prueba encontrada en el exterior, de allí la necesidad que el Estado sea parte de Convenios Internacionales.

> Artículo 39. A nadie se le hará sufrir pena sino por delito, cuasidelito o falta, sancionados por ley anterior y en virtud de sentencia firme dictada por autoridad competente, previa oportunidad concedida al indiciado para ejercitar su defensa y mediante la necesaria demostración de culpabilidad. No constituyen violación a este artículo o a los dos anteriores el apremio corporal en materia civil o de trabajo o las detenciones que pudieren decretarse en las insolvencias, quiebras o concursos de acreedores. (Constitución Política de la Republica de Costa Rica)

Además, teniendo en cuenta el artículo 154 del Código Procesal Penal que establece el procedimiento de emitir exhortos o cartas rogatorias a las autoridades extranjeras, para que sean canalizados por la Secretaria General de la Corte Suprema de Justicia y luego enviadas al Ministerio de Relaciones Exteriores para que sea tramitado por la vía consular.

> ARTICULO 154.-Exhortos a autoridades extranjeras Los requerimientos dirigidos a jueces o autoridades extranjeras se efectuarán por exhortos y se tramitarán en la forma establecida por la Constitución, el Derecho Internacional y el Comunitario vigentes en el país. Por medio de la Secretaría de la Corte Suprema de Justicia, se canalizarán las comunicaciones al Ministerio de Relaciones Exteriores, el cual las tramitará por la vía diplomática. No obstante, en casos de urgencia podrán dirigirse comunicaciones a cualquier autoridad judicial o administrativa extranjera, anticipando el exhorto o la contestación a un requerimiento, sin perjuicio de que, con posterioridad, se formalice la gestión, según lo previsto en el párrafo anterior. (Ley N°7594)

Inclusive se abre la posibilidad que, ante casos de urgencia, se puede anticipar el exhorto, permitiendo que las formalidades de la carta rogatoria se cumplan posteriormente. A nivel institucional a través del Ministerio de Relaciones de Exteriores y Culto, pues es la dependencia administrativa encargada de velar por todo lo correspondiente a la política exterior del país y por ende todas las

gestiones en el extranjero, como lo indica el artículo 1 de la Ley Orgánica del Ministerio de Relaciones Exteriores y Culto.

> Artículo 1º.- El Ministerio de Relaciones Exteriores y Culto, en virtud de las disposiciones constitucionales y legales respectivas, tiene por función colaborar con el presidente de la República, bajo la dirección del Ministro nombrado al efecto, en la formulación sistematizada de la política exterior del país, en la orientación de sus relaciones internacionales y en la salvaguardia de la soberanía nacional. Es el medio por el cual el Estado realiza todas sus gestiones ante Gobiernos e Instituciones extranjeras. (Ley N° 3008)

2.2.4.4 Fundamento Jurídico para la obtención de la prueba a nivel Consular

En el ámbito internacional existe un Convenio Internacional de Viena sobre Relaciones Consulares elaborado el día 26 de abril de 1963 y ratificado por Costa Rica a través de la Ley N° 3767. En este Convenio se habla específicamente de las funciones que tiene la oficina consular y el procedimiento por seguir en relación con las cartas rogatorias como lo dispone el artículo 5 inciso j de la Convención. Al ser el Ministerio de Relaciones Exteriores y de Culto el encargado de la política exterior del país, todos los asuntos oficiales internacionales deben ser canalizados con el Ministerio como vía de conducto.

> ARTICULO 5. Funciones consulares. Las funciones consulares consistirán en: j) Comunicar decisiones judiciales y extrajudiciales y diligenciar comisiones rogatorias de conformidad con los acuerdos internacionales en vigor y, a falta de los mismos de manera que sea compatible con las leyes y reglamentos del Estado receptor. (Ley N° 3767)

Además, se debe tomar en cuenta uno al Código de Bustamante uno de los más antiguos tratados referentes al Derecho Internacional Privado, Costa Rica lo ratificó a través de la Ley N° 50. En este Código lo que regula es todo lo referente con los exhortos y cartas rogatorias en donde se puede llevar a cabo la comunicación entre los países por la vía diplomática de acuerdo al artículo 388 y siguientes del Código de Bustamante.

2.2.4.5 Fundamento Jurídico para la obtención de la prueba por Autoridad Central

2.2.4.6 Convención Interamericana sobre Asistencia Mutua en Materia Penal (Convención de Nassau)

Este Tratado Internacional es una herramienta que elaboro la Organización de Estados Americanos con el fin que todos los Estados Miembros formaran parte de ella. Uno de los ejes de este Tratado es en relación con la asistencia mutua en donde se comprometen todos los Estados a brindar toda la colaboración pertinente para llevar a cabo una investigación criminal, juicios, obtención de prueba en el exterior y actuaciones en materia penal propiamente de conformidad con el artículo 2 del Convenio de NASSAU. Costa Rica ratificó este Tratado a través de la Ley N° 9066 el día 22 de noviembre del 2011.

> Artículo 2. APLICACION Y ALCANCE DE LA CONVENCION. Esta Convención se aplica únicamente a la prestación de asistencia mutua entre los Estados Partes; sus disposiciones no otorgan derecho a los particulares para obtener o excluir pruebas, o para impedir la ejecución de cualquier solicitud de asistencia. (Ley N° 9066)

Además, se establece en el Convenio de Nassau que cada Estado establezca una autoridad central para recibir las comunicaciones de los países, esto permite que el conducto de envió y recibo de pruebas se vuelva ágil. Costa Rica, designó

a la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) como punto de contacto.

2.2.4.7 Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo)

Este tratado internacional fue elaborado por la Organización de la Naciones Unidas (ONU) y fue firmado en diciembre del 2000 por 128 países en una cumbre que se llevó a cabo en Palermo. Uno de los ejes de este tratado radica en el hecho de luchar fuertemente en contra del crimen organizado a través que los Países firmante se comprometieran a tipificar ciertas conductas, luego brindar asistencia judicial reciproca en las investigaciones, procesos, facilitar información y obtener elementos de prueba de acuerdo con el artículo 18 inciso 1 y 2. Este país ratificó este Convenio a través de la Ley N° 8302 el día 27 de junio del 2003. El fenómeno de la ciberdelincuencia se puede considerar como crimen organizado, pues existen bandas a nivel mundial que se dedican a utilizar la tecnología con fines delictivos.

> 1º—Los Estados Parte se prestarán la más amplia asistencia judicial recíproca respecto de investigaciones, procesos y actuaciones judiciales relacionados con los delitos comprendidos en la presente Convención con arreglo a lo dispuesto en el artículo 3 y se prestarán también asistencia de esa índole cuando el Estado Parte requirente tenga motivos razonables para sospechar que el delito a que se hace referencia en los apartados a) o b) del párrafo 1 del artículo 3 es de carácter transnacional, así como que las

> víctimas, los testigos, el producto, los instrumentos o las pruebas de esos delitos se encuentran en el Estado Parte requerido y que el delito entraña la participación de un grupo delictivo organizado. (Ley N° 8302)

Así mismo, en este tratado se estipuló la opción de cada Estado designar una autoridad central esto con el fin que sea el canal de comunicación con los otros países y le de curso, seguimiento a las solicitudes de asistencia judicial internacional correspondiente con delincuencia organizada, de conformidad con el artículo 18 inciso 13 de la Convención de Palermo. Costa Rica, designó a la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) como punto de contacto.

2.2.4.8 Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI)

En el ámbito de la cooperación internacional es un tema sumamente relevante, siendo que uno de los fines del requerimiento de la asistencia es para un auxilio judicial referente a la obtención de elementos probatorios del extranjero y demás hechos. Debido a esta situación, se creó la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) adscrita a la Fiscalía General de la República de Costa Rica.

La creación de este despacho con fines internacionales fue autorizada por el Consejo Superior del Poder Judicial de Costa Rica en la Sesión número 03-2008, artículo LXV, del 15 de enero de 2008, en donde se declaró con lugar la resolución administrativa número 53-2007, ya que era un hecho necesario que fortaleciera la asistencia jurídica internacional dentro del Ministerio Publico. A través de la resolución administrativa 74-2008, se delegó a Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI) la representación de la Fiscalía General de la Republica de Costa Rica, para realizar todo lo tendiente a la cooperación internacional. Además, que a través de la resolución administrativa 167-2008, se ordenó a todas las fiscalías del país que toda gestión de carácter extranjero fuera canalizada por la OATRI.

Dentro las funciones de las OATRI, le corresponde realizar, dar un seguimiento a las solicitudes de asistencia penal internacional, las cartas rogatorias y demás solicitudes internacionales de videoconferencia, es decir, esta oficina es el canal del Ministerio Público en donde pasa todo lo referente a solicitudes de Fiscales cuando requieren prueba del exterior, o una actuación procesal.

Este despacho mantiene la condición de autoridad central de herramientas internacionales como: La Convención de las Naciones Unidas contra la Delincuencia Organizada (Convención de Palermo), La Convención Interamericana sobre Asistencia Mutua en Materia Penal (Convención de Nassau), y el Convenio sobre la Ciberdelincuencia (Convenio de Budapest)

2.2.4.9 Asistencia Jurídica Internacional k

La cooperación jurídica internacional se puede conceptualizar como un auxilio dirigido al Estado Requerido para que ejecute dentro de su jurisdicción un acto procesal, traslado de detenidos, envió de documentos, de información, de elementos de prueba u otras actuaciones de acuerdo con las cláusulas de cada Tratado en específico, es decir, es un mecanismo internacional para solicitarse entre sí una mutua colaboración. Esta asistencia internacional se basa únicamente en principios de buena fe y de cortesía, de cada país para que exista diplomáticamente una ayuda mutua, a posteriori.

De esta manera la asistencia jurídica internacional se clasifica en niveles, considerando el grado de profundización que requiera la asistencia. El primer nivel lo forman actuaciones de mero trámite como notificaciones, intimaciones, comunicaciones en general, los pedidos de un acto de instrucción para una práctica de prueba. Al segundo nivel le corresponden los requerimientos de asistencia para una medida cautelar. El último comprende, la ejecución de sentencias extranjeras. (Gutiérrez, 2010)

De acuerdo con la Pirámide de Hans Kelsen, los Convenios Internacionales cuentan con una mayor jerarquización que las leyes vigentes del país de conformidad con el artículo 7 de la Constitución Política.

Para que la asistencia jurídica internacional sea procedente, debe cumplir una serie de parámetros como primer punto debe existir un Tratado Internacional, como segundo debe establecerse en las cláusulas de tramitología de la solicitud de asistencia, como tercero si los Estados convienen en designar una autoridad central que sería el conducto de comunicación, remplazando las vías consulares o tradicionales, como cuarto el cumplimiento de los requisitos mínimos de forma y fondo de la solicitud de asistencia internacional de conformidad con las disposiciones del Tratado Internacional.

En Costa Rica se cuenta con distintos Tratados Internacionales relacionados a la asistencia jurídica internacional enfocados en la materia penal, como lo es la Convención de las Naciones Unidas contra la Delincuencia Organizada (Convención de Palermo), o la Convención Interamericana sobre Asistencia Mutua en Materia Penal (Convención de Nassau).

2.2.4.10 Procedimiento Consular para la obtención de prueba digital internacional

El procedimiento para obtener prueba del exterior se traduce por medio de los exhortos o cartas rogatorias, esto con el fin de canalizar diplomáticamente la solicitud de cooperación internacional del Estado Requerido. El conducto mediante el cual se deben dirigir los requerimientos de exhortos o cartas rogatorias referentes a la Asistencia Internacional deben enviarse a la Secretaria General de la Corte Suprema de Justicia para canalizarse la comunicación con el Ministerio de Relaciones Exteriores, por medio de la vía diplomática. Por ende, todas estas son reglas de diligenciamiento de cartas rogatorias están fundamentadas en el Derecho Internacional Privado.

Este sistema de comunicación por la vía consular significa una demora para el proceso penal, ya que es un trámite tedioso y engorroso, y al final de cuentas el principio consagrado en el artículo 41 de la Constitución Política, se ve violentado, pues la justicia no está siendo ni pronta ni cumplida. La gestión consular se realiza porque es meritorio para el proceso recolectar esa prueba o esa información del

exterior, por ello esta vía de comunicación diplomática tiende a traer muchas complicaciones para los sujetos intervinientes y operadores del derecho.

2.2.4.11 Procedimiento por medio de Autoridad Central para la obtención de prueba digital internacional

Este moderno medio de comunicación por medio de las autoridades centrales se debe definir como aquellos órganos definidos por los países firmantes del Convenio Internacional. Surge como un conducto de comunicación correspondiente al curso de las solicitudes de cooperación internacional con mucha más rapidez, sustituyendo la forma de comunicación tradicional o consular.

> Las llamadas autoridades centrales surgen a partir de mediados del siglo XX y han cobrado marcado protagonismo en la cooperación institucionalizada. Se trata de organismos encargados de tramitar las solicitudes de cooperación jurídica internacional, agilizando la prestación del auxilio y superando de tal modo la lentitud de los procedimientos ordinarios. (Drehzik de Klor, 2005. p.73)

La designación entre los Estados en el Convenio de fijar una autoridad central permite que el flujo de la información sea mucho más ágil, en esta vía no se requiere que la carta rogatoria se traslade a entidades burocráticas. Únicamente en este medio de comunicación, se requiere que la solicitud de asistencia

internacional cumpla con los requisitos mínimos de forma y fondo acordados en la firma del Tratado. El Convenio de Nassau a modo de ejemplificación exige en la solicitud como requisitos: una breve identificación de los hechos, el delito por el que se acusa, una descripción de la solicitud y el fundamento de la solicitud.

Al ser la OATRI la autoridad central designada tanto en el Convenio de Nassau y el de Palermo, para llevar a cabo todas las gestiones internacionales, el fiscal a cargo de la causa penal deberá solicitarle a la OATRI la colaboración esto con el fin de solicitarle a las autoridades extranjeras un auxilio para obtener prueba digital del exterior de la causa penal.

2.2.4.12 La Prueba Espuria

En doctrina, se le conoce como la Prueba Espuria o la Teoría del Fruto Envenenado aquella forma de obtención de prueba a través de la infracción de un derecho fundamental del imputado y que impide al Juez valorar dicha prueba encadenada de una ilicitud. Esta teoría nació propiamente en Estados Unidos, ya que hubo un caso en donde la Corte Judicial condenó a un sujeto fundamentándose en una intercepción telefónica que le realizaron los Policías, por ello el defensor apeló la decisión judicial basado en la violación a la privacidad, pues la intercepción telefónica se dio sin el consentimiento del otro, por ende, toda la información obtenida de dicha llamada telefónica era ilegal impidiendo la valoración del juez sobre dicha prueba.

Esta teoría del fruto del árbol envenenado lo que pretende es la prohibición de valoración en un litigio de un elemento probatorio, nacido por la violación de un derecho fundamental. A partir de esta teoría supone que toda la prueba declarada espuria, exigirá que la información encadenada a ella también posea el carácter de ilícita.

La teoría de la prueba espuria no es aplicable en tres supuestos en concreto en primer lugar cuando se da una investigación diferente que permite la posibilidad de obtener la prueba de otro modo, ósea, por la teoría de la fuente independiente, como segundo lugar cuando se hubiese descubierto inevitablemente, a esta se le conoce como teoría del descubrimiento inevitable y el último consiste en la teoría de la conexión de antijuricidad o prohibición de valoración.

Que a través una jurisprudencia de un Tribunal de juicio Español acogió el recurso de casación que interpuso el defensor público amparado bajo la Prueba electrónica Espuria en donde indica que, el Tribunal considera prueba ilícita las solicitudes formuladas directamente por la Policía a las compañías Microsoft (de acceso y extracción de datos de los correo electrónicos intercambiados entre Fructuoso Gonzalo, Domingo Ruperto e Ildefonso Nazario, y de datos relativos a las conexiones IP de Gonzalo) y Telefónica (de informe sobre los datos relativos a las conexiones IP respecto a la cuenta de correo electrónico atribuida a Fructuoso Gonzalo) pues dichas solicitudes las habría cursado motu proprio sin obtener la autorización judicial correspondiente (no obra documentada en la causa ninguna autorización judicial previa). Se alude aquí a la nula e irregular obtención de mandamientos e intervención de correos electrónicos y datos asociados. (Oliva, 2016)

Ahora bien, a nivel nacional existen un caso referente a la prueba espuria, en el que corresponde al caso CCSS-Fischel en donde la Sala Tercera de la Corte Suprema de Justicia procedió con la declaratoria de la ilegalidad de la prueba

traída de Panamá, pese a que el Estado Panameño obtuvo la prueba legalmente, sin embargo el Ministerio Público no puede solicitar a través de la solicitud de asistencia internacional información que infrinja el ámbito de privacidad de las cuentas bancarias del sujeto, pues más bien se exige que en Costa Rica el levantamiento de secreto bancario sea ordenado por un juez. La autorización judicial del levantamiento de secreto bancario debe cumplir una serie de parámetros para su procedencia, el primero de ellos exige que la resolución este fundada, luego la individualización de los documentos y el último que debe existir un indicio comprobado, por ello la existencia de un Tratado Internacional en donde se tiene como fin la cooperación mutua de una forma ágil, no se puede prestar para que el ente acusador cometa arbitrariedades al debido proceso. (Voto N° 2011-0499 de la Sala de Casación Penal)

El Código Procesal Penal a través de los artículos 180, 181, 182, 184 regula sobre la legalidad de la prueba, en donde cualquier elemento probatorio que se obtenga por la transgresión de un derecho fundamental el juzgador no debe valorar dicho elemento por nacer de la ilegalidad. Ahora bien, en nuestra Carta Magna en el artículo 40 tutela el hecho que cualquier declaración obtenida por la violencia es nula.

2.2.4.13 El papel de la Sección de Delitos Informáticos

La Unidad de Sección de Delitos Informáticos, se creó en 1997, ya que era necesario el procesamiento de las computadoras en casos importantes, como lo fue el desfalco del Banco Anglo, que se requirió de expertos forenses para la debida recolección de información contenida en un computador, sistema informático. Posteriormente la carga de trabajo fue aumentando, debido al crecimiento de ciberdelitos, por ello el Consejo Superior ordeno la creación de esta Unidad especializada en Delitos Informáticos.

Dentro de los fines que tiene esta Unidad de Sección de Delitos Informáticos del Organismo de Investigación Judicial, es investigar los delitos informáticos realizados en suelo nacional, así como investigar otro tipo de delitos utilizados para la comisión o un medio de prueba, realizar el análisis forense de los teléfonos celulares decomisados a causa de un proceso penal.

La Sección de Delitos Informáticos, realiza a nivel general tres macroprocesos una vez que se incauta un dispositivo móvil o un ordenador, el primer macroproceso que realizan los investigadores es el respaldo de indicios contenidos en un dispositivo de almacenamiento, computadoras, el segundo

macroproceso se conceptualiza como un análisis forense dentro del cual se puede realizar un peritaje de indicios, o el análisis de un sistema informático, y el último macroproceso sería la investigación informática de los ciberdelitos, crimen organizado.

Ahora bien, dentro de los retos que posee la Unidad de Sección de Delitos Informáticos del Organismo de Investigación Judicial sería un mayor fortalecimiento del Laboratorio Forense, un mayor desarrollo y especialización en las áreas de investigación.

Las distintas Policías a nivel mundial, que investigan delitos informáticos deben cumplir con una serie de estándares, esto con el fin de luchar eficientemente contra el cibercrimen, pues el fenómeno de las nuevas tecnologías permite que cada día los delincuentes informáticos, tengan mucho más conocimiento informático para delinquir.

En procura de lograr la oportuna investigación de ciberdelitos, la Policía Nacional de Colombia busca modernizar sus equipos de investigación y de análisis pericial. Sin embargo, se requiere fortalecer constantemente estos equipos especializados, incluyendo la adquisición de herramientas OSINT, el fortalecimiento se basa también en modernizar y actualizar los equipos, mantener al día la licencia de programas forenses y certificar a los expertos policiales que tratan la evidencia al respecto estándares como el ISO 27037 y ISO 27042 dan directrices. La calibración y certificación de laboratorios forenses en informática son otro importante aspecto a considerar. (Bautista, 2018)

En Costa rica, se cuentan con varias herramientas de hardware y software para la preservación y análisis de la evidencia informática. La capacitación técnica y de informática forense es difícil de gestionar debido a los recursos presupuestarios y que está por lo general es limitado, sin embargo, se pide colaboración con otras policías. (Lewis, 2009)

2.2.4.14 Proyecto de Ley N° 21187

Esta propuesta de reforma de ley fue presentado al Plenario Legislativo el día 16 de diciembre del 2018. A través de este Proyecto de Ley, tiene como fin enmendar una serie de errores que contienen las antiguas reformas a la legislación de delitos informáticos n° 9048 y 9135, ya que esta propuesta a reforma viene a conceptualizar de una forma más técnica la tipificación de los delitos informáticos.

Siendo, que las nuevas tecnologías (TICS) avanzan cada día, por ello nuevas conductas delictivas van surgiendo dentro del ciberespacio, se hace necesario que la legislación se encuentre debidamente actualizada. Por ello, a través de este Proyecto de Ley se implementan nuevos tipos penales como el acoso cibernético, la captación de actos o partes íntimas, difusión o tráfico de contraseñas o vulnerabilidades, Ingeniería Social, difusión de noticias falsa, ciberacoso sexual, compras ilícitas mediante tarjetas.

Debido a la ratificación del Convenio de Budapest por parte de Costa Rica, se hace necesario que nuestra legislación cumpla con los parámetros estándar del Tratado Internacional, por ello se incluyó para su tipificación las siguientes conductas que no estaban reguladas en el Código Penal: la primera de ellas es el

acceso ilícito o hacking, en donde este fenómeno ya fue abordado en este trabajo de investigación y el abuso de los dispositivos.

A nivel procesal se cuenta con una serie de dificultades para la investigación de un delito informático como la carencia de un protocolo de actuación para la lucha contra la ciberdelincuencia, luego la falta de cooperación internacional ágil por parte las empresas alojadas en el extranjero, llámese Facebook, Google, Microsoft, Apple, para la obtencion de prueba electrónica. Además, Costa Rica no tiene una Estrategia Nacional en contra de la ciberdelincuencia que permita una lucha eficiente del cibercrimen en nuestro país. Teniendo una cooperación ágil, permitiría descartar o avanzar si la Dirección IP pertenece al autor responsable vinculado al ciberdelito o si simplemente esta conexión fue utilizada como un puente para cometer otro hecho delictivo. (Medrano, 2018)

Dada esta limitación para la obtención de prueba del exterior, se creará una Comisión Nacional para la Lucha contra la ciberdelincuencia, que permita un diálogo con las empresas domiciliadas al exterior, esto con el fin que brinden la información solicitada por Costa Rica.

2.3. HIPOTESIS

2.3.1 Concepto

Según Pardinas (1991), "Hipótesis es una proposición enunciada para responder tentativamente a un problema." (p.151)

Arias (2006)

> Es importante señalar, que, por lo general, la formulación de hipótesis es pertinente en investigaciones de nivel explicativo, donde se pretende establecer relaciones causales entre variables. En las investigaciones de nivel exploratorio y en algunas de carácter descriptivo comúnmente no se plantean hipótesis de explícita, es decir, se trabaja con objetivos. (p.16)

Mejía (2005)

> Las variables de estudio. Pueden contener diferentes tipos de variables dependiendo del nivel de estudio. Así, en un estudio explicativo se podrá tener una o más variables independientes que se asocian a una variable dependiente. En un estudio correlacional se puede decir que se cuenta con

variables predictora o variable antecedente y variable criterio o lo que se predice. (p.46)

2.3.2 Hipótesis de la Investigación

Si la ineficacia a la respuesta por parte de empresas alojadas al exterior para obtener prueba digital de exterior tiene alguna repercusión dentro del proceso penal correspondiente a un delito informático.

2.3.3. Variable independiente

Según Álvarez (2008) la variable independiente es “aquella donde el investigador puede manipular ciertos efectos; en otras palabras, supone la causa del fenómeno estudiado”. (p.59)

Buendía (2001)

> La variable independiente es la que investigador mide, manipula o selecciona para determinar su relación con el fenómeno o fenómenos observados. Esta variable es conocida también como variable estímulo o input. Es una variable que puede tener su origen en el sujeto o en el entorno del sujeto. Es la variable que el investigador manipula para ver los efectos que produce en otra variable. En la relación más si cumple, un investigador estudia qué le sucedería a la variable efecto cuando cambia los valores de la variable causa o variable independiente. (p.38)

Namakforoosh (2005)

> “La variable que el investigador desea explicar se considera como la variable dependiente. La variable que se espera que explique el cambio de

> la variable dependiente es referida como la variable independiente; es decir, la variable dependiente es el resultado esperado de las variables independientes. A las variables dependientes también se les conoce como variables de criterio y a las variables independientes, como variables predictivas. (p.16)

2.3.4. Variable independiente de la investigación

Que la variable independiente de este trabajo es si el ordenamiento jurídico costarricense es suficiente para abordar de una manera adecuada los delitos informáticos contemplando ademas los mecanismos legales para la obtención de la prueba en el extranjero.

2.3.5. Variable dependiente

Buendía (2001)

> La variable dependiente es el factor que el investigador observa o mide para determinar el efecto de la variable independiente o variable causa. La variable dependiente es la variable respuesta o variable salida u output. En términos comportamentales, esta variable es el comportamiento resultante de un organismo que ha sido estimulado. Es el factor que aparece, desaparece, varía, etc., como consecuencia de la manipulación que el investigador hace de la variable independiente. Ala variable dependiente se le considera así porque sus valores van a depender de los valores de la variable independiente. Ella, la variable dependiente, representa la consecuencia de los cambios en el sujeto bajo estudio o en la situación que se está estudiando. (p.41)

Según Álvarez (2008),

la variable dependiente es “el efecto producido por la variable independiente, es decir representa lo que se quiere determinar en forma directa en la investigación” (p.60)

Hayman (1994), define a la variable dependiente como “la propiedad o característica que se trata de cambiar mediante la manipulación de la variable independiente”. (p.28)

2.3.6. Variable dependiente de la investigación

La victimización, “es el resultado de una conducta antisocial contra un grupo o persona; por el cual se deviene en víctima.” (Fattan, 1980, p.5)

La variable dependiente en esta investigación es: La falta de una tutela judicial efectiva para la obtención de la prueba en el exterior ante la investigación de un delito informático no brindada a la víctima.

2.4. OPERACIONALIZACION DE LA HIPOTESIS

Bavaresco (1997)

> Las variables, para que permitan medir los conceptos teóricos, deben llevarse a sus referentes empíricos, es decir, expresarse en indicadores que cumplan tal función, a esa descomposición de la variable en su mínima expresión de análisis, se le ha denominado, proceso de operacionalización. (p.76)

Hipótesis	Conceptos	Variables	Indicadores
Si la ineficacia a la respuesta por parte de empresas alojadas al	Delito Informático	Delito Informático	Ordenamiento jurídico acorde al fenómeno de las nuevas tecnologías.

exterior para obtener prueba digital de exterior tiene alguna repercusión dentro del proceso penal correspondiente a un delito informático.			
	Investigación del delito informático.	Investigación del delito informático.	Evidencia Digital normalmente se encuentra en el extranjero.

CAPITULO III: MARCO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Al ser un tema novedoso y actual, del cual todavía no existen estudios que profundicen sobre la problemática de este trabajo de investigación se enmarca en el tipo denominado exploratoria, al respecto, Arias (2006), indica que “la investigación exploratoria es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir, un nivel superficial de conocimientos.” (p.23)

3.1.1 Finalidad

La finalidad de la investigación tendrá como aporte a una mejora en cuanto a la investigación de un delito informático cuando se solicite obtener de prueba electrónica al exterior correspondiente a las grandes empresas, y se debe tomar en cuenta lo novedoso de esta problemática y lo poco que ha sido estudiado el tema desde una forma científica y formal, por lo tanto la finalidad de esta investigación es la denominada “teórica” la cual según Fox (1981) “se orienta a conocer y persigue la resolución de problemas amplios y de validez general” (p.128).

3.1.2 Dimensión temporal

El alcance temporal de esta investigación se puede situar como transversal, ya que se pretende analizar el impacto actual que tiene dentro de la investigación criminal de un delito informático la no obtencion de evidencia digital alojada en el extranjero correspondiente a las grandes empresas y el análisis jurídico de la legislación costarricense.

Respecto a la dimensión temporal, Hernández, Fernández y Batista (2014) indican que “los diseños de investigación transeccional o transversal recolectan datos en un solo momento, en un tiempo único. Su propósito es describir variables, y analizar su incidencia e interrelación en un momento dado. (p.154).

3.1.3 Marco

El marco de la investigación es aquel que se relaciona con la amplitud del estudio o la profundidad con que se llevara a cabo la investigación y lo que esta abarca, al respecto Arias, F (2006) indica: “el nivel de investigación se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio.” (p.26)

Si se define la profundidad de la investigación en mega, macro y micro, donde la primera estudia una investigación es mega cuando se realiza un estudio nacional acerca de condiciones socioeconómicos y, para esto se aplica una censo en todo el país, o cuando se plantea realizar un análisis administrativo, que incluya recursos humanos, finanzas y mercadeo, entre otras áreas, de toda la empresa o, cuando se plantea analizar una temática amplia y compleja en el campo del derecho laboral como lo indican González & Segura (2018), la segunda como lo referencia lo macro, en cambio, refiere al estudio realizado en una parte o fragmento de lo mega, por ejemplo, un estudio de mercado en una provincia, una evaluación del desempeño laboral en un departamento de una empresa o una evaluación de la didáctica que utilizan los docentes de toda una escuela, o, un análisis jurídico en un campo específico del derecho laboral, por ejemplo, acerca del salario mínimo, González & Segura (2018) y conceptual y la tercera en aspectos específicos, esta investigación es del tipo de denominado macro, pues este estudio abarcó la totalidad de mecanismos legales que tiene Costa Rica para

la obtención de prueba en el exterior y sus posibles repercusiones en el proceso penal.

3.1.4 Naturaleza

La naturaleza de la investigación está divida en 3 tipos: cuantitativa, cualitativa y mixta.

La investigación cuantitativa, según Cortes e Iglesias (2004), “toma como centro de su proceso de investigación a las mediciones numéricas, utiliza la observación del proceso en forma de recolección de datos y los analiza para llegar a responder sus preguntas de investigación.” (p.10)

Respecto a la investigación cualitativa, indica Gurdian (2007) “El propósito de las técnicas cualitativas es la obtención de información fundamental en las percepciones, creencias, prejuicios, actitudes, opiniones, significados y conductas de las personas con que se trabaja”. (p.179)

La investigación mixta para Hernández, Fernández y Batista (2014), “implica un conjunto de procesos de recolección, análisis y vinculación de datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento del problema”. (p.532)

Es menester indicar que sobre este proyecto de investigación es meramente cualitativo, por ende, todo lo que se estudio fue a través de opiniones, percepciones de especialistas en la materia para verificar si el ordenamiento jurídico es suficiente para luchar eficazmente en contra de la ciberdelincuencia, así como de los mecanismos legales para obtener evidencia digital del extranjero proveniente de las grandes empresas y su problemática para la recolección.

3.1.5 Carácter

El carácter de la investigación hace referencia a 4 grandes tipos de estudio: exploratorios, descriptivo, correlacionales y explicativos.

Los estudios exploratorios son más flexibles, más amplios y dispersos que otros estudios, los descriptivos tienen como objetivo especificar características, propiedades y rasgos del fenómeno analizado; por su parte los correlacionales evalúan la relación existente entre 2 o más conceptos, categorías, variables, en un contexto particular; los estudios explicativos encuentran las razones o causas que provocan ciertos eventos, sucesos o fenómenos.

Respecto a la investigación exploratoria, esta es la categoría en la que se ubica este estudio, según Hernández, Fernández y Batista (2014) “se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes.” (p.91)

Este trabajo se puede describir como exploratorio, ya que el derecho informático y sobre todo este tema de investigación es de suma novedad, pues no existe un trabajo que aborde de manera sistemática, la problemática a nivel

procesal con la que hoy se cuenta, esto es con relacion a la no obtencion de evidencia digital en el exterior de forma ágil perteneciente a las grandes empresas y su repercusión en el proceso penal.

3.2 SUJETOS Y FUENTES DE INVESTIGACIÓN

Este apartado, hace referencia a las personas con un estudio profundo del cibercrimen sobre las cuales se hace el estudio. En esta investigación los sujetos de estudio son profesionales especialistas en ciberdelincuencia y un Fiscal del Ministerio Público que a lo largo del documento se han mencionado. Respecto a los sujetos de información, indica Barrantes (2005) “la población es el conjunto de elementos que tienen características en común” (p. 135).

En cuanto a las fuentes de información estas son aquellas de donde se extrae la información para efectuar el estudio.

Hernández, Fernández y Batista (1991), citando a Dankhe

> Las fuentes primarias o directas son aquellas que proporcionan información de primera mano, se pueden considerar los libros, las revistas, los periódicos, los artículos, las monografías y las tesis. Las fuentes secundarias son compilaciones, resúmenes y listados de referencias de fuentes primarias publicadas en un área de conocimiento en donde se mencionan y discuten artículos, libros, tesis, entre otros. Por último, las

fuentes terciarias son documentos que compendian nombres y títulos de revistas, boletines, conferencias, simposios, etc.

3.2.1 Fuentes de primera mano

En este estudio, las fuentes de investigación de primera mano fueron las leyes consultadas, proyectos de ley, Convenios Internacionales y cinco tesis que estudiaron el fenómeno de la ciberdelincuencia.

Las tesis consultadas son las siguientes

Título	Universidad	País	Año
Problemática del Delito Informático: Hacia una necesaria regulación internacional	Universidad de Costa Rica	Costa Rica	2010
La impunidad de los delitos informáticos en la cibersociedad costarricense	Universidad de Costa Rica	Costa Rica	2010
Los delitos informáticos y su tipificación en la Legislación ecuatoriana	Universidad de Loja	Ecuador	2012
Delitos Informáticos-Caso de Estudio	Instituto Polytechnic Nacional	México	2011
Daños Informáticos del artículo 264 del código Penal y propuesta de reforma	Universidad Complutense	Madrid	2013

Además, las fuentes secundarias que se utilizaron en este trabajo de investigación fueron libros, artículos referentes al Derecho Informático en general, luego autores que hablan de una posible aplicación de una prueba electrónica

envenenada o espuria y de libros relacionados con la cooperación internacional para la lucha en contra de la ciberdelincuencia.

Título	Autor	País	Año
Delitos Informáticos.	C. Chinchilla	Costa Rica	2004
El Impacto Social de la Informática Jurídica en México.	J. Téllez	México	1996
Ciberdelitos.	Poder Judicial de la Provincia de Salta.	España	2013
Trámites judiciales internacionales.	A. Drehzik de Klor	Argentina	2005
La Prueba Electrónica Envenenada.	R. Oliva	España	2016

Y por último las fuentes terciarias que se utilizaron en este trabajo de investigación fueron una serie de conferencias que brindaron los especialistas en delitos informáticos.

Título	Conferencista	País	Año
Perspectivas Jurídicas e Informáticas. I ciclo de conferencias de Derecho informático, realizado en San José, Costa Rica el día 09 de octubre del 2015.	A. Medrano	Costa Rica	2015
El fenómeno de la delincuencia informática desde una perspectiva internacional. Simposio Internacional, realizado el 08 de octubre del 2015.	C. Chinchilla	Costa Rica	2015

3.3.1 La población

La población, según Moráguez (2006), “es el conjunto de todos los individuos, objetos, procesos o sucesos homogéneos que constituyen el objeto de interés. La población se relaciona directamente con el campo de estudio"

Esta investigación se enfoca principalmente en que la evidencia digital normalmente requiere de cooperación internacional para la obtención de prueba esto con el fin de incorporarla al proceso penal. Así las cosas, la población que se relaciona al campo de estudio sería el proceso penal y los mecanismos para recoger prueba del exterior.

3.3.2 La muestra

Batthyany K, Cabrera M. (2011).

> Una muestra es un subconjunto de la población compuesto por las unidades que efectivamente se observan, y representan a las otras unidades de la población que no se observan. Existen diversas maneras de seleccionar una muestra, dependiendo de los objetivos y la estrategia que se utilice en la investigación

En este tema en investigación, la muestra nace a partir de las víctimas de los delitos informáticos en donde dichas conductas delictivas cometidas en el ciberespacio deben ser investigadas por las autoridades competentes.

3.3.3 No probabilística

Castro (2003).

> En la muestra no probabilística, la elección de los miembros para el estudio dependerá de un criterio específico del investigador, lo que significa que no todos los miembros de la población tienen igualdad de oportunidad de conformarla.

En esta investigación, lo que se pretende es conocer si existe una relación directa entre la obtención evidencia digital del exterior y la investigación de un delito. Se involucran únicamente los delitos informáticos que se cometen en el ciberespacio.

3.4 TÉCNICAS E INSTRUMENTOS PARA DESARROLLAR LA INVESTIGACIÓN

Las técnicas cualitativas, según Rodríguez, Flores y García (1996) “estudian la vida social en su propio marco natural, sin distorsionarla ni someterla a controles experimentales. Su objetivo es captar y reconstruir significados a través de procesos, comportamientos y actos de hechos sociales.

Tal como lo indica Lindlof (1995), “el investigador cualitativo busca conservar la forma y contenido del comportamiento humano para finalmente analizar estas cualidades.

Rodríguez, Flores y García (1996).

> El lenguaje de las técnicas cualitativas es conceptual y simbólico ya que, a pesar de que se basa en preguntas fijas, las respuestas no están basadas en escalas numéricas. El modo de captar información es flexible y desestructurado. No lleva un orden riguroso ni un método exclusivo. Esto permite modificar la investigación dependiendo de los intereses del investigador. Su manera de recopilar información es inductiva, es decir, parte de hechos particulares para llegar a una conclusión teórica

Ante este panorama, se desprende que este tipo de investigación abre un abanico de opiniones de especialistas en delitos informáticos, policías internacionales y criterios de fiscales que amplían e interpretan de una gran manera la problematización de la ciberdelincuencia y su carácter transfronterizo.

Y para Buendía, Colás y Hernández (2001)

> La entrevista es una técnica que consiste en recoger la información mediante un proceso directo de comunicación entre entrevistador y entrevistado en el cual responde a cuestiones, previamente diseñadas en función de las dimensiones que se pretenden estudiar planteadas por el entrevistador.

La técnica utilizada en este trabajo de investigación fue la entrevista, en donde a partir de juicios de valor por parte de un fiscal, policía internacional y un profesional especialista en la ciberdelincuencia, se pudieron conocer las posturas de cada uno de ellos en relación directa al cibercrimen como un fenómeno delictivo de la actualidad.

3.4.1 La investigación documental

La investigación documental juega un papel esencial en cualquier proyecto, pues ayuda a entender los acontecimientos históricos, espaciales y temporales que rodean un estudio.

Tal como lo indica Lindlof (1995). “Un investigador puede usar está técnica para irse familiarizando con la problemática que estudia y detectar posibles escenarios y estrategias:”

Hernández, Fernández y Batista (2000)

> La investigación documental consiste en: detectar, obtener y consultar la bibliografía y otros materiales que parten de otros conocimientos y/o informaciones recogidas moderadamente de cualquier realidad, de manera selectiva, de modo que puedan ser útiles para los propósitos del estudio.

La investigación documental en este estudio fue de tipo documental y bibliográfica, en donde se consultaron las leyes, proyectos de ley, libros referentes

a delitos informáticos, revistas, artículos de doctrinarios especialistas en ciberdelincuencia.

3.4.2 Estudio de caso

El estudio de caso, según, Mertens (2005) es “una investigación sobre un individuo, grupo, organización, comunidad o sociedad, que es visto y analizado como una entidad.”

Para Hernández, Fernández y Batista (2014), citando a Blatter (2008) quien define al estudio de caso como “una aproximación investigativa en la cual una o unas cuantas instancias de un fenómeno son estudiadas en profundidad.”

Esta investigación, concretamente se estudió si nuestro marco jurídico es suficiente para atender los ciberdelitos y luego que repercusión existe durante la investigacion criminal de un delito informático, cuando la evidencia digital está en el extranjero.

3.5 DEFINICIÓN CONCEPTUAL, OPERATIVA E INSTRUMENTAL DE LAS VARIABLES

3.5.1 Definición conceptual

Según González y Segura (2018), “refiere a la claridad teórica de la variable y se extrae del marco teórico, se indica cual definición se utiliza en esta investigación. La misma definición del capítulo II.”

El análisis del cuerpo jurídico de la ciberdelincuencia se puede conceptualizar ante el apogeo de las nuevas tecnologías, se hace necesario que el Estado tipifique dichas conductas, por ello se debe analizar si es suficiente.

Efecto legal: la consecuencia jurídica, sería que los ciudadanos se les brinde una tutela judicial efectiva, y que no quede como letra muerta, sino que sea posible aplicarlo a nivel sustantivo y procesal.

3.5.2 Dimensión

Para esta investigación, se definieron las siguientes categorías de análisis como variables de interés:

- Aplicabilidad de la normativa
- Evidencia digital se encuentra en el extranjero.
- Beneficios para la colectividad en la investigacion criminal.

3.5.3 Definición conceptual de la dimensión

A continuación, se presenta la definición conceptual de la dimensión de este estudio:

- Aplicabilidad de la normativa: se puede determinar como la esfera jurídica en donde el Estado debe contemplar y aplicar todas las sanciones penales ante las conductas delictivas provocadas por un medio informático.

- Evidencia digital en el extranjero: se analizan las consecuencias del fenómeno de las nuevas tecnologías (TICS) al no poseer fronteras, la evidencia siempre se encuentra en otro país.

- Beneficios para la colectividad durante la investigacion: este estudio permitiría entender de una mejor manera la problemática durante la investigacion esto con el fin que se dé una tutela jurídica que permitiría indicar que nuestro país es un Estado de Derecho, conforme a la salvaguarda de derechos fundamentales.

3.5.4 Definición operacional

Según González y Segura (2018), “refiere a traducir en indicadores que permitan la observación directa de la variable; es decir, la observación empírica donde la medición se realiza en aspectos concretos””

Como primera variable, se puede considerar el análisis jurídico de la normativa sobre la ciberdelincuencia debido al fenómeno de las nuevas tecnologías (TICS)

Como segunda variable, se mencionó que debido a que el Internet no posee fronteras, la investigacion de un delito informático radica en el extranjero y de igual manera la prueba.

3.5.5 Definición Instrumental

Según González y Segura (2018), se especifican las técnicas e instrumentos por utilizar para la recolección de la información; según las variables abordadas y los resultados esperados, se indican las preguntas que miden los indicadores de las variables".

En esta investigación se utilizó como técnica de recolección de información, la entrevista en donde permite a los expertos dar un criterio con peso de acuerdo con su experiencia profesional ante el fenómeno de la ciberdelincuencia.

3.5.6 Cuadro de operacionalización de las variables:

Objetivo específico	Hipótesis	Variable	Definición Conceptual	Definición Operacional	Definición Instrumental
Explorar la totalidad de leyes y normativas existentes para determinar a ciencia cierta la carencia del delito Hacking.	Si la ineficacia a la respuesta por parte de empresas alojadas al exterior para obtener prueba digital de exterior tiene alguna repercusión dentro del proceso penal correspondiente a un delito informático.	Delito Informático	El análisis del cuerpo jurídico de la ciberdelincuencia se puede conceptualizar ante el apogeo de las nuevas tecnologías, se hace necesario que el Estado tipifique dichas conductas, por ello se debe analizar si es suficiente.	Como primera variable, se puede considerar el análisis jurídico de la normativa sobre la ciberdelincuencia debido al fenómeno de las nuevas tecnologías (TICS).	Entrevista
Realizar un análisis del derecho comparado en la región de Latinoamérica y España con relación a la tutela de ciberdelitos que se dan.		Investigación del delito informático.	Efecto legal: la consecuencia jurídica, sería que los ciudadanos se les brinde una tutela judicial efectiva, y que no quede como letra muerta, sino que sea posible aplicarlo a nivel sustantivo y procesal.	Como segunda variable, se mencionó que debido a que el Internet no posee fronteras, la investigacion de un delito informático radica en el extranjero y de igual la manera la prueba.	Entrevista
Desarrollar un análisis de los mecanismos legales que posee las autoridades competentes para la consecución de solicitar prueba al exterior a la luz de las distintas normativas y la posible aplicación de la Teoría de la prueba espuria. --- Determinar los instrumentos de investigación informáticas que posee la entidad investigadora en Costa Rica, para la recolección de prueba digital en la lucha en contra de la					Entrevista

ciberdelincuencia, junto con las limitantes que cuenta la Policía Judicial.					

4. ANALISIS E INTERPRETACION DE DATOS

4.1 Entrevista a la Licenciada Sharon Segura de la Fiscalía de Fraudes del I Circuito Judicial de San José.

1. ¿De qué sirve contar con la mejor legislación sino se puede hacer valer a nivel procesal en cuanto a la obtencion de prueba digital del exterior?

En realidad, independientemente del proceso, la Fiscalía tiene muchos problemas en obtener la evidencia del exterior por los canales diplomáticos, ya que las legislaciones son diferentes, evidentemente va a existir alguna incompatibilidad en cuanto donde se pide la información. En Facebook, se tiene mucho problema de si tenemos suerte que contesten, lo hacen cuando la causa está a punto de prescribir o del todo no contestan, es complicado.

2. ¿Cuántos Fiscales a cargo en esta oficina de ejercer la acción penal de los ciberdelitos?

Estamos a cargo 6 Fiscales.

3. ¿Según su criterio, usted me podría indicar si en Costa Rica se marca la brecha a nivel de Latinoamerica en relación con la tutela de los ciberdelitos?

He ido a varios cursos en donde he tenido la oportunidad de estar con otras personas de otros países, y usted ve las legislaciones de los otros países y no son ni la cuarta parte de lo que Costa Rica tiene en el código Penal o los tipos penales de los otros países son más ligeros, pero no sientan como un capítulo de Delitos Informáticos como nuestro Código Penal. Ahora bien, depende de cada en caso en concreto, tener una tutela judicial efectiva, porque puede contener las dificultades citadas arriba.

4. ¿Una vez que se ratificó el Convenio de Budapest, el Ministerio Público ha solicitado información al exterior?

Ese dato lo maneja la Oficina de Asesoría Técnica y de Relaciones Internacionales (OATRI) que es la encargada de ello.

5. ¿Qué tan importante es la cooperación internacional para demostrar la culpabilidad del ciberdelincuente?

Es de total relevancia.

6. ¿Según su criterio y expertiz han existido ocasiones en donde las empresas estadounidenses como Apple, Google, Facebook han denegado la solicitud de cooperación para brindar información?

No le puedo dar un dato exacto, ya que todo se canaliza por la Oficina de Asesoría Técnica y de Relaciones Internacionales (OATRI).

7. ¿Considera que los jueces de la República tienen el conocimiento del fenómeno del cibercrimen?

   Al inicio le parece que eran muy ajenos a la ciberdelincuencia, pero ahora en las capacitaciones se están tomando más cuenta, ya que se ocupa que todos estemos en la misma sintonía.

4.2 Entrevista a Freddy Bautista en su condición de Oficial de la Reserva Activa de la Policía Nacional, Criminalista y Auditor Forense de Colombia.

1. ¿Usted podría indicar las herramientas forenses con que cuenta la policía de Colombia, da pie para luchar en contra de la ciberdelincuencia?

Las herramientas forenses con las que cuenta la Policía de Colombia para luchar contra la ciberdelincuencia son: herramientas de análisis de malware, herramientas de análisis de vulnerabilidades de sistemas informáticos Herramientas de recuperación y análisis de evidencia digital de dispositivos móviles y de data volátil, igualmente para se dispone de herramientas de análisis de grandes volúmenes de datos big data, Herramientas de disección de malware y Herramientas sandbox para identificar el comportamiento de malware.

2. ¿Dentro de su expertiz, cuando se requiere evidencia digital al exterior a Facebook, Google, Microsoft, se complica la investigación del ciberdelito, se presenta la misma problemática que en C.R?

Se presenta la misma situación, cuando se requiere petición a proveedores como Facebook, Microsoft, Twitter, para lo cual ellos tienen un protocolo de atención a peticiones judiciales. Lo más importante es que las autoridades de

Policía Judicial y Ministerio Publico o Procuraduría, tengan canales autorizados para hacer estas peticiones, estas compañías han dispuesto de contactos para acceder a la información, lo complejo es que la misma se limita a datos biográficos de creación y de conexión, pero esos datos dado el mercado ilegal de datos personales en Internet, puede ser fácilmente suplantados o falsos.

3. ¿La Policía de Colombia o las autoridades competentes recurren a canales informales para la obtención de prueba en el exterior?

Para la obtención de dicha información se utilizan los canales formales y que disponen a disposición los proveedores internacionales, acompañados de la ordena policía judicial cuando aplica. Existen dos rutas: Una de ellas es a carta rogatoria, la cual procede su trámite a través de la cancillería o ministerio de relaciones exteriores, este trámite suele tardar meses, y es en la práctica poco efectivo. La segunda opción es la de procurar MLAT (Tratado de Cooperacion Mutua) con algunos países, y acudiendo a ello contactar autoridades homologas y agilizar las solicitudes, otro mecanismo que viene cobrando mucha importancia es el de hacer uso de EUROPOL e INTERPOL como instancias de cooperación policial internacional.

4. ¿Dentro de su experiencia, el material tecnológico que mantiene la Policía de

Colombia, cumple con los standards internacionales para investigar los ciberdelitos?

En procura de lograr la oportuna investigación de ciberdelitos, la Policía Nacional de Colombia busca modernizar sus equipos de investigación y de análisis pericial. Sin embargo, se requiere fortalecer constantemente estos equipos especializados, incluyendo la adquisición de herramientas OSINT (Open Source Intelligence o Inteligencia de Fuentes Abiertas), así como el fortalecimiento se basa también en modernizar y actualizar los equipos, mantener al día la licencia de programas forenses y certificar a los expertos policiales que tratan la evidencia al respecto estándares como el ISO 27037 y ISO 27042 dan directrices. La calibración y certificación de laboratorios forenses en informática son otro importante aspecto a considerar.

5. ¿Qué aspecto considera que es fundamental para luchar eficazmente en contra de la ciberdelincuencia?

Varios son los factores fundamentales para luchar contra el cibercrimen:

-La cooperación de los sectores público/privados con las agencias de ley

-La cooperación internacional

-El fortalecimiento tecnológico para investigar las nuevas modalidades de cibercrimen

Y finalmente una normatividad robusta que fundamente el actuar de las autoridades

Judiciales.

6. ¿A modo de conclusión, Cuales serían las limitantes que tendría la Policía de Colombia y sus posibles puntos de mejora, ¿si lo hay?

Básicamente las acciones de mejora de la Policía Nacional radican en el fortalecimiento de talento humano, capacidades técnicas y de herramientas tecnológicas para perseguir las nuevas modalidades de cibercrimen y de delitos conexos tales como lavado de dinero, narcotráfico, amenazas.

Garantizar la permanencia del talento humano y lo más importante es mantener la presencia en instancias de formación continua e intercambio de buenas prácticas globales.

4.3 Entrevista al Licenciado José Adalid Medrano, Especialista de Delitos Informáticos y Co-redactor de las reformas n°9048, n°9135 al Código Penal.

1. ¿Por qué nace el Proyecto de Ley N°21187?

Nace porque hemos detectado en la práctica que falta capacitación por parte de la Fiscalía para comprender que es un delito informático, cuáles son las conductas tipificadas en el código Penal. Por otro lado, también encontramos que existen limitaciones a la hora obligar a las empresas que brindan servicios electrónicos de brindar la información expedita, tomando en cuenta que las empresas privadas, suelen durar a un mes medio a dos meses, para entregar datos de tráfico. Cuando enfrentamos a un delito informático lo normal es que, si comete a través una plataforma tecnológica, y ocupemos de empresas como Facebook que brinden la dirección IP. Esto permitiría agilizar avanzar o descartar si la IP pertenece o no al ciberdelincuente, lo que genera actualmente es impunidad en la investigación. Ya que al no contar con dicha información supone un desistimiento de la causa por falta de elementos probatorios.

3. ¿Se requiere que las grandes empresas como Google, Facebook, le brinden la información a Costa Rica de forma ágil?

De hecho, todas estas empresas brindan plataformas tecnológicas para dar esa información, pero van a requerir que lo solicite una autoridad competente para hacerlo, quiere decir, que, si Costa Rica se exige que sea por una orden de un juez, ahora si Costa Rica permite que Policía Judicial lo haga, dichas empresas lo van a permitir. Que pasa, que a través del Proyecto de Ley N°21187, se indica que ciertos datos van a poder ser solicitados por la Policía Judicial, Ministerio Publico o una orden del juez, sin embargo, si el proveedor de servicio de acuerdo con sus políticas de privacidad le ha pedido la autorización a las personas para que estos datos puedan ser facilitados, a las autoridades en el marco de una investigación criminal se le puedan dar inclusive a la Policía Judicial. Ahora, lo que va a permitir la Comisión Nacional de Lucha contra la ciberdelincuencia, es que agreguen dentro de las políticas de privacidad el permiso del usuario para la facilitación.

4. ¿Cuál es el mecanismo para solicitar prueba digital del exterior?

Hay datos que pueden ser solicitados mediante una plataforma tecnológica que tiene la Policía, debidamente autenticado. Ahora, los datos de contenido u otros datos se hacen a través de los mecanismos que están habilitados para eso, entonces si la empresa coopera con un MD, y si no hay otra forma de hacerlo sería por la carta rogatoria. Por ejemplo, en un curso que se impartió en Argentina, en donde personeros de Facebook se encontraban allí, nos indicaron que para

Argentina solicitamos que el Juez, revise una serie de cuestiones mientras que en Costa Rica, dicha empresa extranjera no nos lo pide de esa manera. Luego, hay que entender que Facebook, Google, Whatsapp, actúan bajo principios de buena fe, ya que no están obligados a cooperar. Únicamente están obligados cuando existe una solicitud de una autoridad de los Estados Unidos de América. Y con respecto a delitos que no están contemplados en Estados Unidos como la difamación, injuria, calumnia hecha por las plataformas tecnológicas no brindan la información, ya que en dicho país no es delito, únicamente es penado con responsabilidad civil, por ende, ante dichos delitos no brindan cooperacion.

5. ¿Actualmente no hay ningún registro o informe de las grandes empresas extranjeras, en donde se indique cuantas veces han facilitado información a otros Estados?

Ellos, deben de tener informes internos. Lo que nosotros requerimos es que a través de un reporte han existido tantos casos y se han cooperado en tantas causas, sin dar datos de ninguna persona, únicamente con fines estadísticos. Y si algún dato puede ser comprometido que lo omitan del informe. El tema es contener estadísticas en cuanto a cooperacion internacional como en temas de investigación, inclusive ya con la creación de la Comisión Nacional de Ciberdelincuencia, se le podría solicitar que hagan un apartado únicamente de Costa Rica.

6. ¿Estas grandes empresas a la hora que le llegan solicitudes de Asistencia Internacional, realizan preferencias de países?

Lo que se ha dicho con el Convenio de Budapest, es que, si bien es cierto, ellos no toman ninguna preferencia de cual país haya ratificado el Convenio, lo que si es cierto es que pertenecer a Budapest permite tener un marco normativo claro sobre delitos informáticos y sobre un país que respeta la libertad de expresión. Lo que genera un perfil mucho mejor para inclusive llegar acuerdos o tener algún tipo de trato preferencial con estas compañías, en donde a cada país les ponen reglas diferentes.

7. ¿Dentro de su experiencia, ha visto que se solicite el sobreseimiento definitivo en causas de delitos informáticos por falta de elemento probatorios?

Es que es algo muy común que no obtengan la prueba, entonces se desestima la causa. Inclusive, peor todavía que la Fiscalía no solicita dicha prueba digital porque supone que no se las van a dar, en algunos casos por atipicidad o porque no pudieron obtener información. Y estas desestimaciones, las hacen en volumen prácticamente.

5.CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se concluye a través de un estudio de Derecho Comparado a nivel de Latinoamérica y España, que la legislación penal costarricense de delitos informáticos es una norma modelo para todos los países de la región.
- Se concluye, que de un estudio de la normativa penal la legislación no tipifica la conducta de Acceso Ilícito o Hacking.
- Se concluye que, del estudio detallado, Costa Rica no cuenta con la debida cooperacion internacional de las grandes empresas a la hora de brindar evidencia digital o en su caso datos de abonado.
- Se concluye que las respuestas de las plataformas tecnológicas en Estados Unidos, ante una solicitud de evidencia digital de Costa Rica deviene en ineficaz en el tanto que nunca contestan a las autoridades costarricenses.

- Se concluye que la Sección de Delitos Informáticos, no cuenta con los suficientes instrumentos tecnológicos para la investigacion informáticos debido a una falta de recursos presupuestarios y falta de personal forense
- Se concluye que no funciona de nada contar con la mejor legislación de delitos informáticos a nivel sustantivo, si no es posible accesar a la evidencia digital por parte de los administradores de las plataformas tecnológicas que se domicilian en los Estados Unidos de América que permitan demostrar la culpabilidad del delincuente informático.

5.2 RECOMENDACIONES

- Se recomienda que Costa Rica establezca una Política exterior dirigida a los Estados Unidos de América, esto con el fin que dichas plataformas tecnológicas colaboren en el marco de una investigacion de un delito informático.
- Se recomienda que la Asamblea Legislativa apruebe el Proyecto de Ley N° 21187, ya que contiene el tipo penal hacking, nuevas figuras penales y hasta herramientas procesales que permiten la facilitación la investigacion de un delito informático cuando se requiere evidencia del exterior.
- Se recomienda una mayor capacitación sobre los ciberdelitos a los Fiscales, Jueces y Defensores Públicos, para una debida administración de

Justicia, al ser una materia tan técnica requiere de un conocimiento constante.

- Se recomienda que el Poder Judicial dote de mayor presupuesto a la Sección de Delitos Informáticos, para que cuente con las herramientas de investigación de último nivel y asigne mayor personal a la Unidad.

BIBLIOGRAFÍA

Acurio del Pino, S (2008) *Delitos Informáticos: Generalidades.* Madrid, España.

Adalid Medrano, *Entrevista*, 19 de diciembre del 2018.

Arias, F (2006). *El proyecto de investigación: Introducción a la metodología científica*. 5º. Ed. Venezuela: Episteme.

Anguita, J. (2017). *"Análisis Histórico Jurídico de la Lucha contra la ciberdelincuencia en la Unión Europea"* Revista de Estudios en seguridad internacional, Vol. 4, No 1 (2018): 107-126

Alcivar Trejo, C.; Álvarez Domenech, G. y Ortiz Chimbo, K.; (2016) *"La Seguridad Jurídica frente a los Delitos Informáticos*" Revista de Investigacion Jurídica. 10 (12): 41-57.

Álvarez Venegas R.; Paredes Hernandez, L. y Arteaga Pérez J.; (2015) *Guía Metodológica para la elaboración de proyectos de investigación*, México.

Álvarez, W (2008). *La Naturaleza de la Investigación*. Caracas: BIOSFERA

Asamblea legislativa, Proyecto de Ley 14.097, Reformas al código Penal,03-06-2001, Comisión Especial de Redacción, San José.

Asamblea Legislativa, Informe Jurídico, N°18.484, de Aprobación del Convenio de Budapest, 03-03-17, Comisión Especial de Área Jurídica, San José.

Asamblea Legislativa, *Proyecto de Ley N° 18546 REFORMA DE LOS TIPOS PENALES ESTABLECIDOS EN LOS ARTÍCULOS 167, 196, 196 BIS, 231, 236 Y 288 DEL CÓDIGO PENAL*. Publicado en el Diario Oficial La Gaceta 26 de abril del 2013.

Barrantes, R. (2005). *Investigación un camino al conocimiento, un enfoque cualitativo y cuantitativo*. Costa Rica, EUNED.

Batthyany K, Cabrera M. (2011). *Metodología de la investigación en Ciencias Sociales.* Uruguay: UCUR.

Bavaresco, A. (1997). *Proceso metodológico en la investigación*. Maracaibo: Ediluz.

Bernal, C. (2010). *Metodología de la Investigacion administración, económica, humanidades y ciencias sociales.3ra ed. Colombia. Editorial Pearson.*

Buendía, L.; Colás, P. y Hernández, F. (2001): *Métodos de investigación en Psicopedagogía*. Madrid: McGraw-Hill.

Buompadre J, (2017). *Sexting, Pornovenganza, Sextorsion*. Argentina, Buenos Aires. Recuperado de: http://www.pensamientopenal.com.ar/system/files/2017/11/doctrina46005.pdf

Castro, M. (2003). *El proyecto de investigación y su esquema de elaboración*. 2 Ed. Caracas: Uyapal.

Campoli G. (2003) *Derecho Penal Informático* 1a ed. San José: Ed. Investigaciones Jurídicas S.A

Centro de Información Jurídica en Línea. (2006). *Delitos Informáticos*. 1era edición. San José: Ed: Universidad de Costa Rica.

Código Penal Federal de México. (2018) Disponible en: http://www.indaabin.gob.mx/leyinfo/marco/Compilacion/cpfederal.doc

Código Penal Guatemalteco. (2018). Decreto No. Guatemala. Recuperado de:http://www.oas.org/juridico/mla/sp/gtm/sp_gtm-int-text-cp.pdf.

Cortés Cortés M, Iglesias León M (2004). *Generalidades sobre Metodología de la Investigación*. México: E

Consejo de Europa. (2010) *Informe Explicativo*. 1ra ed.

Consejo de Europa (2001). *Convenio sobre la Ciberdelincuencia*. Budapest. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Constitución Política de Costa Rica, La Gaceta, San José, 08 de noviembre de 1949.

Chinchilla C. (2004). *Delitos Informáticos*. 1era. Edición. San José: Ed. Investigaciones Jurídicas.

Chinchilla, Carlos. (2010) *Respuesta al oficio número 076-2010 sobre Reforma a varios capítulos del código Penal adición de una nueva sección denominada Delitos Informáticos y Conexos*. Manuscrito no publicado.

Data Protection and Cybercrime División del Consejo de Europa. (2013). *Guía básica para Fuerzas y Cuerpos de Seguridad Jueces y Fiscales*, ed. Estraburgo: Consejo de Europa.

Derechos Digitales. (2018). *Derechos Humanos y Tecnología en América Latina. Disponible* en: https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/

Derechos Digitales. (2017) *La necesidad de legislar sobre Cibercrimen en Panamá*. Paraguay. Recuperado de: https://www.derechosdigitales.org/12378/la-necesidad-de-legislar-sobre-cibercrimen-en-panama/

Drehzik de Klor, A. (2005). *Trámites judiciales internacionales*. Buenos Aires, Argentina: Editorial Víctor P. de Zavalía S.A

De la Cuadra, F. (2002). *Virus Informáticos*. España. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/1029432.pdf

De la Mata, N. (2009) *El delito de daños informáticos: Una tipificación defectuosa*. España. Recuperado de: https://minerva.usc.es/xmlui/bitstream/handle/10347/4149/07.Mata.pdf;sequence=

Erick Lewis, *Entrevista*, 29 de setiembre del 2009.

Fattan, A. (1980). *Regards sur; a victimologie, criminologie. Les presses se I´* Université de Montreal, Canadá.

Freddy Bautista, *Entrevista*, 06 de diciembre del 2018.

FLÓREZ, R. y TOBÓN, A (2003). *Investigación educativa y pedagógica*. Bogotá, Colombia.

Fox J, (1981). *El proceso de investigación en educación*. Pamplona: EUNSA

Gallego, A. (2012). *Delitos Informáticos: Malware, Fraudes y Estafas a través de la red y como prevenirlos*. Tesis inédita para optar el grado de Licenciatura en Derecho. Universidad Carlos III de Madrid, España.

González J. (2013) *Daños informáticos del artículo 264 del Código Penal y propuesta de reforma*. (Tesis inédita de Doctorado de Derecho) Universidad Complutense de Madrid, España

González Vallejo L.; Guerra Vargas, G. y Jara Ocampo, A.; (2018) *Manual de Normas A.P.A citas y referencias bibliográficas. Costa Rica:* Universidad Hispanoamericana.

González Vallejo, L.; Chinchilla Jiménez A; Guerra Vargas, G y Jara Ocampo, A.; (2018) *Guía cuantitativa para trabajo finales de graduación tesinas y tesis en ciencias sociales.* 2-18 ed. Llorente: Universidad Hispanoamericana

GUANIPA, M. (2008) *Objetivos de investigación en las ciencias sociales*, Madrid, España. Recuperado de: **http://Gestiopolis.com**

Guardiola, M. (2016). *Los nuevos delitos tras la reforma del Código Penal*. Madrid, España. Recuperado de: http://www.legaltoday.com/practica-juridica/penal/penal/los-nuevos-delitos-informaticos-tras-la-reforma-del-codigo-penal

Gómez, A. (2010) *"El delito informático, su problemática y la cooperación internacional como paradigma de su solución".* Redur. 1(3): 169-203

Gurdián, A. (2007) *El paradigma cualitativo de la investigación socio-educativa* (Coordinación Educativa y Cultural Centroamericana. Costa Rica: Printcenter

Henao de Yepes, L. (1991) *Delitos y contravenciones*. Colombia. Recuperado de:http://webcache.googleusercontent.com/search?q=cache:3mHt2qUF7pYJ:publicaciones.eafit.edu.co/index.php/nuevo-foro penal/article/download/4076/3329/+&cd=18&hl=es&ct=clnk&gl=cr&client=firefox-b-ab

Hayman, E. (1994). *Investigación documental, técnicas y procedimientos*. Bogotá: Panapo.

Hernández Sampieri R, Fernández Collado C. y Batista Lucio P. (2014). *Metodología de la Investigación*. 6 Ed. México: McGraw Hill

Laboratorio Eset Latinoamérica (2012). *La Historia del Malware*. Recuperado de http://www.esetla.com/pdf/prensa/informe/cronologia_virus_informaticos.pdf.

Lindlof, T.R. (1995). *Qualitative communication research methods.* USA: Sage

López A. y Torres M. (2010) *Problemática del Delito Informático: Hacia una necesaria regulación internacional*. (Tesis inédita de Licenciatura en Derecho) Universidad de Costa Rica, San José

Lemaitre R. (2010) *La impunidad de los delitos informáticos en la cibersociedad costarricense en el ámbito del derecho penal*. (Tesis inédita de Licenciatura en Derecho) Universidad de Costa Rica, San José.

Ley N° 7557. Ley General de Aduanas. La Gaceta, N° 212, 08 de noviembre del 1995, San José, Costa Rica.

Ley N°4755. *Código de Normas y Procedimientos Tributarios*., La Gaceta, N° 117, 04 de junio de 1971, San José Costa Rica. Reformado por el artículo 2º de la ley No.7900 de 3 de agosto de 1999.

Ley N° 9048. Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal, Publicada La Gaceta N°214 del 06 de noviembre del 2012.

Ley N°8968. *Ley de la Protección de la Persona frente al Tratamiento de sus datos personales*. La Gaceta. San José, Costa rica, 05 de setiembre del 2011.

Ley N° 14. *Código Penal de Panamá.* La Gaceta, Panamá, 26 de abril del 2010.

Ley N° 558. *Proyecto de Ley de Modificación y Adición al Código Penal relacionados al Cibercrimen*. Asamblea Nacional de Secretaria General. Panamá. 27 de setiembre del 2017.

Ley N° 7425. Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones. San José, La Gaceta, 08 de setiembre del 1994.

Ley N° 26388. *Reforma al Código Penal de Argentina*. Buenos Aires, Argentina, Diario Oficial, 25 de junio de 2008.

Ley N° 11179. *Código Penal de Argentina*. Buenos Aires, Argentina, Diario Oficial, 21 de diciembre del 1984.

Ley N° 1/2015. *Reforma al Código Penal de España*. Madrid, España, Boletín Oficial del Estado, 31 de marzo del 2015.

Ley N° 9452. Aprobación del Convenio de Europa sobre la Ciberdelincuencia. San José, Costa Rica, La Gaceta, 03 de julio del 2017.

Ley N°1273. *Reformas al Código Penal de Colombia*. Bogotá, Colombia, La Gaceta, 05 de enero del 2009.

Ley N° 63. Reforma al Código Penal Italiano. Roma, Italia, Diario, 12 de mayo del 2018.

Ley N° 88-19. Código Penal de Francia. Paris, Francia, Diario, 05 de enero de 1988.

Ley N° 9452. *Aprobación de Convenio de Budapest*. San José, Costa Rica, La Gaceta, 26 de mayo de 2017.

Ley N° 8039. *Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual.* San José, Costa Rica, La Gaceta, 12 de octubre del 2000.

Ley N° 7594. *código Procesal Penal*, La Gaceta, San José, 04 de junio de 1996.

Ley N° 3008. *Ley Orgánica de Relaciones Exteriores y Culto*, La Gaceta, San José, 18 de julio de 1962.

Ley N° 3767. *Convención de Viena sobre Relaciones Consulares*. La Gaceta, San José, 03 de noviembre de 1966.

Ley N° 50. *Convención de Derecho Internacional Privado - Código de Bustamante*. La Gaceta, San José, 06 de diciembre de 1930.

Ley N° 9006. *Convención Interamericana sobre Asistencia Mutua en Materia Penal (Convención de Nassau).* La Gaceta, San José, 22 de noviembre del 2011.

Ley N° 8302. *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Convención de Palermo*). La Gaceta, San José, 27 de junio del 2003.

Mateos I. (2013) *Ciberdelincuencia Desarrollo y Persecución Tecnológica* (Tesis inédita de Licenciatura de Derecho) Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Madrid, España.

Matellanes, N. (2008) *"Vías para la tipificación del acceso ilegal a los sistemas informáticos".* Revista Penal de la Universidad de Salamanca. 1(22): 50-68.

Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. Revista Chilena de Derecho. Volumen 44 (1): 235-260

Medrano, Adalid (2015). *Perspectivas Jurídicas e Informáticas*. I ciclo de conferencias de Derecho informático, realizado en San José, Costa Rica el día 09 de octubre del 2015.

Mejía, E (2005) *Metodología de la investigación científica.* 1º. Ed. Lima: CEPRE

Mertens, D. (2005). *Research and Evaluation in Education and Psychology. Integrating Diversity with Quantitative, Qualitative, and Mixed Methods*. 2° Ed. USA: SAGE

Ministerio de Ciencia, Tecnología y Comunicaciones (2017) *Estrategia Nacional de Ciberseguridad de Costa Rica. San José, Costa Rica*. Recuperado de: https://micit.go.cr/images/imagenes_noticias/10-11 2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf

Ministerio de Justicia. (2015). *Análisis De Derecho Comparado sobre ciberdelincuencia, ciberterrorismo y ciberamenzas al menor*. Ed. Madrid, España.

Poder Judicial de la Provincia de Salta. (2013). *Ciberdelitos*. 1era edición. Ed España, La salta.

Namakforoosh, M (2005). *Metodología de la Investigación*. 2º. Ed. México. Limusa.

Prensa Libre. (2005) *Delitos Informáticos y su aumento*. La Prensa Libre.

Organismo de Investigación Judicial, Sección de Delitos Informáticos. (2017). *Inicio de la Sección*. Disponible en: https://sitiooij.poder-judicial.go.cr/index.php/comunicacion/noticias/avisos-y-noticias policiales/ítem/3864-seccion-de-delitos-informáticos.

Organismo de Investigacion Judicial. *Sección de Delitos Informáticos y su información*. Brochure.

Pardinas, E (1991). *Metodología y técnicas de investigación en ciencias sociales*. (32a ed.). México: Siglo Veintiuno.

Posada, R. (2006). *"Aproximación a la criminalidad informática en Colombia*". Revista de Derecho, Comunicaciones y Nuevas Tecnologías. 2 (1) 11-60.

Proyecto de Ley N° 21187. *Ley para combatir la ciberdelincuencia*, San José, Costa Rica, 16 de diciembre de 2018.

Real Academia Española. (2017) *Diccionario*. España, Madrid. Real Academia Española. Disponible en: http://dle.rae.es/?id=3DoiQ7S.

Riofrio A. (2012) *Los delitos informáticos y su tipificación en la legislación ecuatoriana*. (Tesis inédita de Magister en Ciencias Penales de Derecho) Universidad de Loja, Ecuador.

Rubí A. (2011) *Delitos informáticos-Casos de Estudio* (Tesis inédita de Maestría en Ingeniería en Seguridad y Tecnologías de la Información) Instituto Politécnico Nacional, México.

Rodríguez Gómez G, Gil Flores J, García Jiménez E (1996): *Metodología de la investigación cualitativa.* España: Aljibe.

Sala Tercera de la Corte Suprema de Justicia. *Voto número 446-F-92*, de las quince horas cuarenta minutos, del veinticinco de septiembre de mil novecientos noventa y dos.

Sala Tercera de la Corte Suprema de Justicia. *Voto número 2006-00763*, de las nueve horas veinte minutos del dieciocho de agosto de dos mil seis.

Sala Constitucional de la Corte Suprema de Justicia. *Voto número 2007-18486*, de las dieciocho horas y tres minutos del diecinueve de diciembre del dos mil siete.

Sala Tercera de la Corte Suprema de Justicia. *Voto número 2001-00074*, de las diez horas con diez minutos del diecinueve de enero de dos mil uno. San José, Costa Rica, 2001.

Sala Tercera de la Corte Suprema de Justicia. *Voto número 2011-0499*, de las a las once horas cuarenta y cinco minutos del once de mayo del dos mil onceo. San José, Costa Rica, 2011.

Sánchez, Z. (2017). *Análisis de la Ley 1273 y la evolución de la Ley con relacion a los delitos informáticos en Colombia*. Colombia. Recuperado de: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11943/1/1053323761.pdf

Sarzana, C (1979) *Criminalità E Tecnologia En Computers Crime*. Rassagna Penitenziaria E Criminologia. Nos. 1-2. Año 1. Roma, Italia.

Sharon Segura, Entrevista, 26 de octubre del 2018.

Secretaria de la Corte Suprema de Justicia. (2010). Acta de Corte Plena en la sesión número 30-2010. San José, Costa Rica. Recuperado de: https://secretariacorte.poderjudicial.go.cr/index.php/component/phocadownload/category/100

Tamayo, M. (2012) *El Proceso de la Investigación Científica*. México: ed. Limusa

Tribunal de Apelación de Sentencia Penal del II circuito judicial de San José. *Voto Numero 2016-0450* de las catorce horas quince minutos, del veintiocho de marzo de dos mil dieciséis.

Tribunal de Apelación de Sentencia Penal del II circuito judicial de San José. *Voto número 2016-0450* de las catorce horas quince minutos, del veintiocho de marzo de dos mil dieciséis.

Téllez, J. (1996) *El Impacto Social de la Informática Jurídica* en México. Segunda Edición, México: Mc Graw Hill REVISTAS

United Nations Office Drugs and Crime. (2013) *Estudio Exhaustivo sobre el delito cibernético*. Ed Nueva York

Visión Criminológica y criminalística. (2013). La suplantación de identidad de tipo físico y de telecomunicaciones como nueva manifestación de las conductas antisociales. México. Recuperado de: http://revista.cleu.edu.mx/new/descargas/1301/articulos/01_La_suplantacion_de_identidad_de_tipo_fisico,_informatico_y_de_telecomunicaciones_como_nueva_manifestacion_de_consductas_antisociales.pdf

GLOSARIO

ANEXOS

ANEXO 1

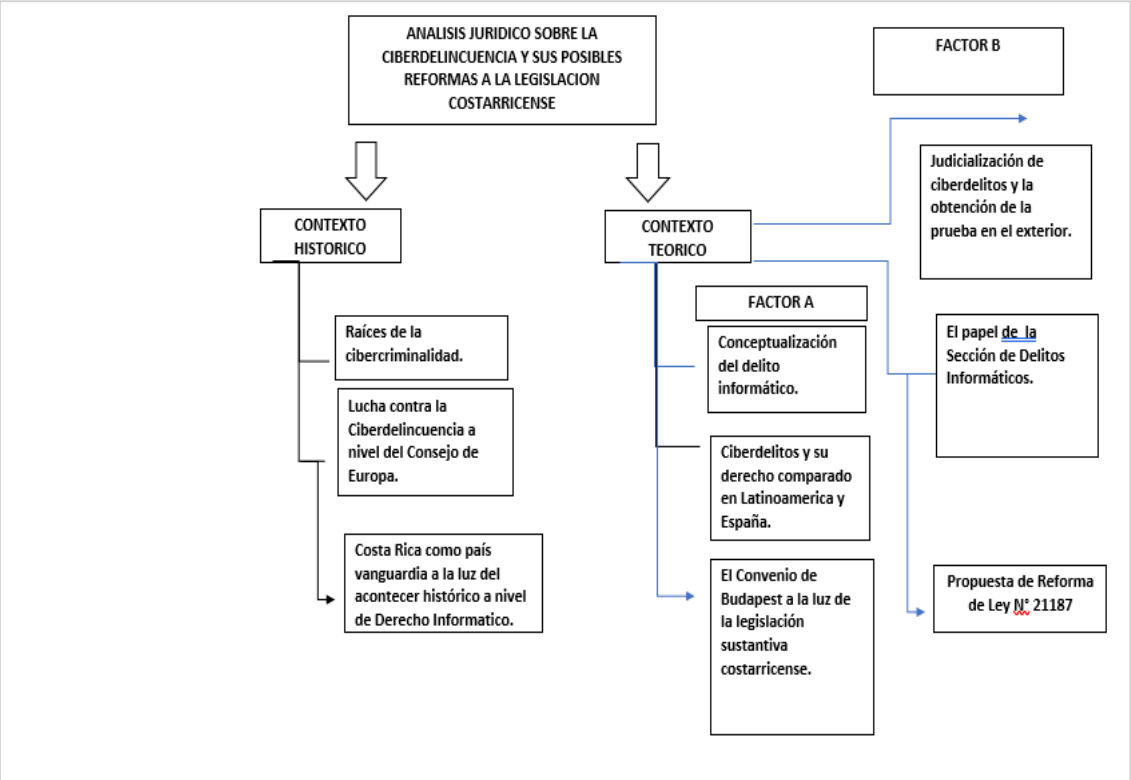
Cuadro Sinóptico

TÍTULO: Análisis jurídico sobre la Ciberdelincuencia y sus posibles reformas a la legislación costarricense **PLANTEAMIENTO DEL PROBLEMA** ¿Es suficiente el ordenamiento jurídico costarricense para enfrentar los fenómenos de la ciberdelincuencia? ¿Desde la perspectiva criminalística nuestras autoridades cuentan con las técnicas y mecanismos efectivos para la obtención de elementos probatorios, ya que este fenómeno del cibercrimen depende de la cooperación internacional para la investigación? **OBJETIVO GENERAL** Determinar la efectividad o la ineficacia con que cuenta las autoridades competentes para solicitar y recabar evidencia digital en el exterior con relación a los proveedores de servicio alojados en otros países, para tener una tutela judicial efectiva.	**OBJETIVOS ESPECIFICOS** Explorar la totalidad de leyes y normativas existentes para determinar a ciencia cierta la carencia del delito Hacking. Realizar un análisis del derecho comparado en la región de Latinoamérica y España con relación a la tutela de ciberdelitos que se dan. Desarrollar un análisis de los mecanismos legales que posee las autoridades competentes para la consecución de solicitar prueba al exterior a la luz de las distintas normativas y la posible aplicación de la Teoría de la prueba espuria. Determinar los instrumentos de investigación informáticas que posee la entidad investigadora en Costa Rica, para la recolección de prueba digital en la lucha en contra de la ciberdelincuencia, junto con las limitantes que	**CONCLUSIONES** - Se concluye a través de un estudio de Derecho Comparado a nivel de Latinoamerica y España, nuestra legislación penal de delitos informáticos es una norma modelo para todos los países de la región. - Se concluye, que de un estudio de la normativa penal nuestra legislación no tipifica la conducta de Acceso Ilícito o Hacking. - Se concluye que, del estudio detallado, Costa Rica no cuenta con la debida cooperacion internacional de las grandes empresas a la hora de brindar evidencia digital o en su caso datos de abonado. - Se concluye que las respuestas de las plataformas tecnológicas en Estados Unidos, ante una solicitud de evidencia digital de Costa Rica deviene en ineficaz en el tanto que nunca contestan a las autoridades costarricenses. - Se concluye que la Sección de Delitos Informáticos, no cuenta con los suficientes instrumentos tecnológicos para la investigacion informáticos debido a una falta de recursos presupuestarios y falta de personal forense - Se concluye que no funciona de nada contar con la mejor legislación de delitos informáticos a nivel sustantivo, si no es posible accesar a la evidencia digital por parte de los administradores de las plataformas tecnológicas que se

	cuenta la Policía Judicial.	domicilian en los Estados Unidos de América que permitan demostrar la culpabilidad del delincuente informático.
FACTOR A: QUE LA VARIABLE INDEPENDIENTE DE ESTE TRABAJO ES SI EL ORDENAMIENTO JURÍDICO COSTARRICENSE ES SUFICIENTE PARA ABORDAR DE UNA MANERA ADECUADA LOS DELITOS INFORMÁTICOS CONTEMPLANDO ADEMAS LOS MECANISMOS LEGALES PARA LA OBTENCION DE LA PRUEBA EN EL EXTRANJERO.	**FACTOR B:** LA FALTA DE UNA TUTELA JUDICIAL EFECTIVA PARA LA OBTENCION DE LA PRUEBA EN EL EXTERIOR ANTE LA INVESTIGACIÓN DE UN DELITO INFORMÁTICO NO BRINDADA A LA VÍCTIMA.	

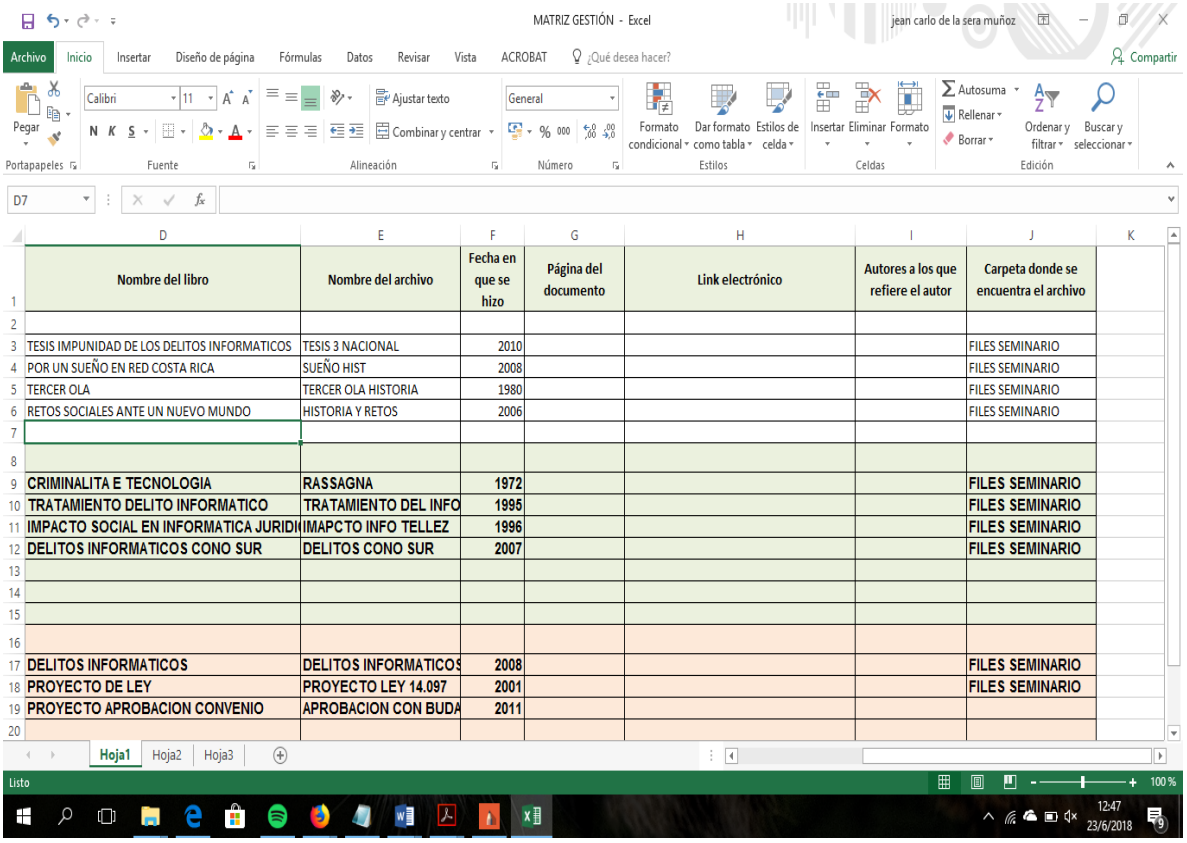
ANEXO 2

Mapa Conceptual borrador



ANEXO 3

Matriz de Gestión



ANEXO 4

Cuadro 2

Fase 1.	Recoleccion de la informacion	¿Cuál seria el análisis jurídico de la ciberdelincuencia y sus posibles reformas a la legislación costarricense?	Observacion Natural	El análisis de la normativa jurídica de la ciberdelincuencia, dentro de sus alcances y deficiencias en el marco legal costarricense.	Deficiencias en el bloque de legalidad.
		1. Explorar la totalidad de leyes y normativas existentes con relación a los ciberdelitos y sus principales carencias a nivel legal. 2. Determinar las falencias de la sociedad en cuanto al tema de ciberseguridad en dispositivos tecnológicos. 3. Sustentar de una forma muy específica sus posibles reformas a la legislación costarricense, de acuerdo al estudio jurídico-social, en busca de tutelar el bien jurídico.			
		Si la aplicación y adaptación de un nuevo y actualizado marco punitivo-informativo tiene alguna incidencia en cuanto a la cibercriminalidad en nuestro país.		La victimización de las personas por la carencia de una protección legal a nivel informático.	Efectos en las posibles reformas y creación de nuevos delitos conforme a la legislación costarricense.
Fase 2.	Observacion	registro de datos	Guion		
Fase 3.	Finalizacion	revisar informacion	concluir con los objetivos de la investigacion		

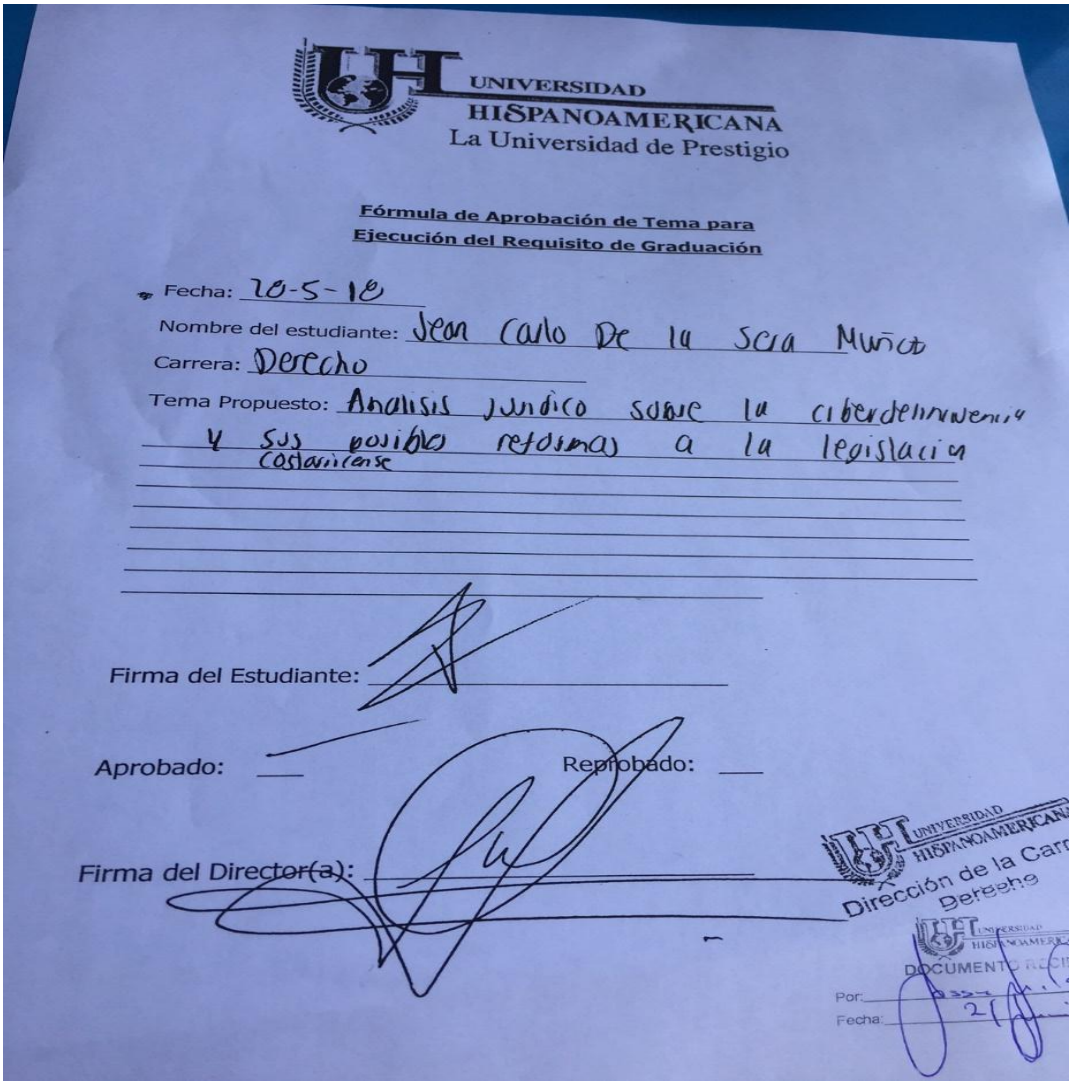
ANEXO 5

Borrador del Instrumento

Variables	Indicador	Instrumento	N° de pregunta	Se le aplica a	Observaciones
El análisis de la normativa jurídica de la ciberdelincuencia, dentro de sus alcances y deficiencias en el marco legal costarricense.	Deficiencias en el bloque de legalidad	entrevista	1	Normativa	
La victimización de las personas por la carencia de una protección legal a nivel informático.	Efectos en las posibles reformas y creación de nuevos delitos conforme a la legislación costarricense.	Entrevista	2	Proyecto de Ley	

ANEXO 6

Hoja de Aprobación del Tema



UNIVERSIDAD HISPANOAMERICANA
La Universidad de Prestigio

Fórmula de Aprobación de Tema para Ejecución del Requisito de Graduación

Fecha: 20-5-18

Nombre del estudiante: Jean Carlo De la Sota Muñoz

Carrera: Derecho

Tema Propuesto: Analisis Jurídico sobre la ciberdelincuencia y sus posibles reformas a la legislación costarricense

Firma del Estudiante:

Aprobado: ___ Reprobado: ___

Firma del Director(a):

UNIVERSIDAD HISPANOAMERICANA
Dirección de la Carr
Derecho

DOCUMENTO RECI
Por:
Fecha:

Anexo 7

Rúbrica del Seminario

UNIVERSIDAD HISPANOAMERICANA DE COSTA RICA SEDE: Llorente **SEMINARIO DE GRADUACIÓN II Q-18**				
NOMBRE DEL PROYECTO: Analisis jurídico sobre la ciberdelincuencia y sus posibles reformas a la legislación costarricense				
NOMBRE DEL ESTUDIANTE: Jean Carlo De la Sera Muñoz				
CARNÉ:LL 13004679		1 a 2 errores	0-error	
ÁREA DE EVALUACIÓN.	PORCENTAJE	50%	100%	OBSERVACIONES
Portada	2			
Agradecimientos y dedicatorias (con indicaciones i, ii).	2			
Tabla de contenidos elaborada con la Herramienta Word (incluyendo los agradecimientos y dedicatorias i,ii)además del protocolo).	2			
Antecedentes del problema. 5 tesis.	5			
Planteamiento del problema (Apoyada en autores).	5			
Abordaje de la Justificación (con base en los cinco elementos de Sampieri).	5			
Formulación del problema. Pregunta.	5			
El Objetivo general, congruencia con los objetivos específicos.	5			
Alcances (Descriptivos, explicativos, social, económico, académico o a la elección del Investigador) Limitaciones (con mayor enfasis en aspectos metodológicos).	4			
Esquema del Marco Teórico, (MAPA CONCEPTUAL), de acuerdo a la carrera (Marco situacional, Contexto Histórico, Contexto Teórico).	5			
Antecedentes de la Investigación (al menos 5 tesis en orden cronológico (3 Internacionales), (2 nacionales) con similitud al tema u objetivos.	5			
Planteamiento de la hipótesis (si va a utilizar).	5			
Operacionalización de la Hipótesis.	5			
Estructura y elaboración del Marco Metodológico: Paradigma, enfoque, tipo Investigación.	5			
Población, población de estudio, muestra, elección de tipo de muestra y procedimiento para llegar a las unidades para aplicación del instrumento.	5			
Espacios físico y temporal, sujetos y fuentes Técnicas de recolección de la Información debidamene estructurado(a).	5			
Definición conceptual, operativa e instrumental de las variables.	10			
Bibliografía aplicando APA (no menor de 20 libros) además de otras fuentes.	10			
Aplicación de la Normativa APA en todo el documento (Versión 6ta) CITAS.	10			
CALIFICACIÓN FINAL	**100**			
Apreciaciones para el tutor:				
NOMBRE DEL TUTOR METODOLOGÍCO : Luis González Vallejo.			**FIRMA**	

DECLARACIÓN JURADA

Yo Jean Carlo De la Soa Muñoz, mayor de edad, portador de la cédula de identidad número 1-1600-0163 egresado de la carrera de Derecho de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura, juro solemnemente que mi trabajo de investigación titulado: Analisis juridico de la ciberdelincuencia y sus posibles reformas a la legislacion costarricense, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los 24 días del mes de enero del año dos mil diecinueve.

Firma del estudiante

Cédula: 1-1600-0163

Tibás, 26 de febrero del 2019.

Señor:

Piero Vignoli Chessler.

Director Carrera Lic. En Derecho.

Universidad Hispanoamericana.

Estimado señor:

El suscrito, en mi condición de profesor de la Universidad Hispanoamericana, le informo que he procedido a efectuar la lectura del trabajo final de graduación titulado **"ANÁLISIS JURÍDICO SOBRE LA CIBERDELINCUENCIA Y SUS POSIBLES REFORMAS A LA LEGISLACIÓN COSTARRICENSE",** elaborado por el estudiante Jean Carlo de la Sera Muñoz, para optar por el título de Licenciatura en Derecho.

Me complace informarle que dicha tesis cumple totalmente con las exigencias académicas establecidas por la Universidad. Además, la elaboración de la misma así como los planteamientos del estudiante, resultan un aporte valiosísimo a la ciencia jurídica, pues viene a llenar un vacío de conocimiento legal sobre el tema, exponiendo aspectos actuales sobre la materia tratada.

Cuenta con mi total aprobación.

Marco Mairena Navarro

Profesor

CARTA DE REVISION FILOLÓGICA

Miércoles 27 de febrero, 2019

Universidad Hispanoamericana
Facultad de Derecho

Estimados señores:

Por este medio yo, Karol Jiménez García, mayor, casada, filóloga y profesora de español, incorporada al Colegio de Licenciados y Profesores, con el número de carné: 039257, vecina de Desamparados, portadora de la cédula de identidad 1-1101-0902, hago constar:

1. Que he revisado el trabajo final de graduación para optar por el grado académico de Licenciatura denominado: **"Análisis jurídico sobre ciberdelincuencia y sus posibles reformas a la legislación costarricense".**
2. Que el trabajo final de graduación es sustentado por el estudiante: Jean Carlo De la Sera Muñoz
3. Que se le han hecho las correcciones pertinentes en acentuación, ortografía, puntuación, concordancia gramatical y otras del campo filológico.

En espera de que mi participación satisfaga los requerimientos de la Universidad Hispanoamericana, se suscribe atentamente,

Karol Jiménez García
Máster
Carné No. 039257
Filóloga