UNIVERSIDAD HISPANOAMERICANA

CARRERA DE DERECHO

TESIS PARA OPTAR EL GRADO DE LICENCIATURA EN LA CARRERA DE DERECHO

CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAÍS ANTE LA FALTA DE REGULACION ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURÍDICAS

Sustentante:
Edwin Pérez Brenes

TUTOR:
Licenciado German Salazar Santamaría

II SEMESTRE, 2019

ÍNDICE

Contenido

DEDICATORIA

A mi madre Marielos Brenes por apoyarme en cada momento de mi carrera, en momento difíciles siempre conté con su apoyo, tanto personal como en mi vida profesional, a los profesores que me brindaron su ayuda y guía durante este periodo para formar de mi un buen abogado, a los compañeros con que compartí muchas clases y que se convirtieron en amistades de las cuales deseo destacar a Nathalia Borbón que durante todos estos años conté con su gran apoyo.

AGRADECIMIENTO

Gracias a la vida por permitirme estudiar y vivir una experiencia tan gratificante como es convertirme en un profesional del Derecho, gracias a cada profesor de esta universidad que formo parte de este proceso integral de formación, gracias a todos los que compartieron momentos buenos y malos en este proceso dentro y fuera de las aulas conmigo. No fue sencillo el camino, pero gracias a sus aportes y apoyo, lo complicado de lograr esta meta se notó menos. Agradezco a todos aquellos que creyeron en mí, familia y amigos, y de los que tomaron parte de su valioso tiempo para mirar esta tesis.

Generalidades

La globalización del ciberdelito es más que un acontecimiento exclusivamente económico, incluye extractos sociales, políticos, y culturales. Procesos de globalización han existido a lo largo de la historia de la humanidad, pero a la actual la identifican la digitalización y las redes de comunicación; por ello mismo, se afirma que vivimos en la era de las tecnologías de la información.

El amplio desarrollo de estas tecnologías, además de ofrecer matices positivos, también contiene aspectos negativos, tales como: conductas antisociales y delictivas, que se manifiestan de formas que hasta ahora no era posible imaginar, ya que muchas de ellas atentan contra el patrimonio de las personas así como de las empresas, debido a que pasan de ser delitos de tipo tradicional, a formas no tradicionales.

En este contexto, la realización de cualquier tipo de trámite o actuación, por parte de una persona física, dirigida a cumplir con sus necesidades en una comunidad creciente y conectada a una multiplicidad de servicios electrónicos como en el sector bancario, de servicios de salud, de servicios públicos, o del comercio, hace que parte relevante de esa información sea constituida por datos de índole personal, que es el motivo de un progresivo desarrollo de normativa centrada en la correcta protección de los mismos.

En términos generales, existen alteraciones cometidas mediante el manejo de medios informáticos, falsificaciones electrónicas, las modificaciones de programas o datos, y el acceso no autorizado a servicios y sistemas informáticos, por lo que muchas empresas tienen que invertir en programas que son cada vez más costosos y sofisticados para la protección de equipos de redes que disminuyan el peligro, y que además no garantizan una protección total. Este conjunto de factores y actos delictivos ponen en manifiesto que, enfrentar este tipo de amenazas cibernéticas, no es una tarea fácil, se requiere de una cultura de seguridad informática, y que como características principales, tenga como prioridad la sensibilización sobre el problema, la responsabilidad, la respuesta oportuna, la estimación de los riesgos, la implementación de los instrumentos de protección y seguridad así como la debida integración de penas a las personas jurídicas en el marco legal costarricense, como lo aconseja el Convenio de Budapest.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

1.1.1 Antecedentes del problema

“societas delinquere non potest” "la sociedad no puede delinquir" es un factor en general, que los países iberoamericanos siguen siendo cómplices de la no responsabilidad penal de las personas jurídicas desde hace ya varias décadas. El escenario económico-empresarial de la criminalidad, marcado por la expansión de la tecnología y por las complejas estructuras jerárquicas y funcionales de las empresas, por ende, nos ofrece cuestiones de particular índole en lo que concierne a la acusación de un hecho ajeno, realizado por un subordinado, administrador u órgano directivo, lo cual acarrea la falta de una disciplina legal más detallada en Costa Rica, debido los novedosos desafíos planteados por el llamado ciberdelito que carece todavía de una adecuada precisión científica que atienda, por lo menos aproximadamente, a las exigencias de control de la intervención penal, sin embargo, los esfuerzos dogmáticos emprendidos principalmente en Alemania y en España, han contemplado un redimensionamiento de los criterios de imputación, con especial énfasis en los fundamentos de los deberes de garantía, lo cual lleva a uno de los primeros y más importantes ataques en la historia de Internet, se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afectó a una computadora, el cual mostraba un mensaje en los equipos infectados, por lo que si no causaba daño alguno, fue la base para el

desarrollo de ataques posteriores con pérdidas multimillonarias, como se menciona en el sitio web de la INTERPOL.

En vista de que la realidad siempre termina imponiéndose sobre el derecho, la ley debe adecuarse y responder a estos desafíos y nuevas formas delictivas del mundo cibernético. En Costa Rica, el Código Penal data del año 1970, y pese a sus diversas reformas parciales, es necesario de una actualización metódica, moderna, conforme con la realidad actual, para que sus principios se ajusten a esta nueva ola global. Por fortuna y sin duda, la reforma más notable recientemente, en el ámbito del ciberdelito, lo fue la efectuada al Código Penal, mediante la Ley 9048 del 10 de julio del 2012, que reformó algunos delitos, creó figuras nuevas o configuró formas de agravación cuando sean cometidos utilizando un sistema de red informática o telemática. Sin embargo, pese a esta reforma legislativa, el país se encuentra aún en deuda, al no contemplar en su legislación sanciones a los entes colectivos que mencionaba la Convención sobre la Ciberdelincuencia o Convenio de Budapest (en lo sucesivo CEC), del 23 de noviembre del 2001.

Aunque hay que reconocer que la Asamblea Legislativa realizó una importante decisión, al aprobar más adelante, en segundo debate, la adhesión de Costa Rica al Convenio que se tramitó como el expediente legislativo número 18.484, y tiene incluso, rango superior a la legislación, según el mandato del artículo 7 de la Constitución Política y la jurisprudencia de la Sala Constitucional, que tiene como objetivo primordial crear una política penal que sea destinada a proteger a la

población frente a la ciberdelincuencia, suscitada por la digitalización y la globalización de las redes.

Según Francisca H. de Canales en su obra metodología de La investigación año 2007 página 262: “todo hecho anterior a la formulación del problema que sirva para aclarar, juzgar e interpretar el problema planteado, constituye los antecedentes del problema”.

Por estos elementos mencionados anteriormente, como la digitalización global y el desarrollo de tecnologías delictivas, debe legislarse sobre delitos relacionados no solo con la privacidad y confidencialidad de los datos y sistemas informáticos, sino también sobre la responsabilidad que tiene los entes colectivos o personas jurídicas. A su vez, se encuentran interesantes razonamientos que deberían darse en el derecho penal, del cual es necesario un estudio y análisis del mismo, pues como ya se conoce y se da tradicionalmente en el derecho penal clásico, la culpabilidad recae sobre la persona o individuo, esto lleva a plantear y analizar la posibilidad de imponer sanciones, para que exista una armonización jurídica dentro del marco legal costarricense. Como se menciona en el Convenio, cuando este tipo de delitos son realizados por cualquier persona física, en su condición de miembro o representante de la persona jurídica; y en especial, responsabilidad penal y civil a las plataformas sociales y proveedores de redes sociales, que muchas veces ellos mismos, sin tomar acción propia, forman parte de manera cómplice de los actos y situaciones que se suscitan en estos ambientes de interacción social.

Ronald Salazar (2002, pág. 199) manifiesta que se crea un clima de impunidad, pues "…la investigación y asignación de responsabilidad de las personas físicas se diluye al amparo de la persona jurídica, en lo que lo único cierto es que en la empresa sirven personas que han actuado en su nombre y realizaron hechos ilícitos, lo que debería llevar a conceptualizar dichas organizaciones en categoría de autor". Según este autor, "…la máxima *societas delinquere non potest* se ha convertido en un producto semántico para eximir de responsabilidad penal de estas corporaciones ha sido quienes se escudan tras ellas" (ibid. Pag. 200).

A nivel local, en Costa Rica debe existir una discusión de este tema que permita estudiar los principios, tales como: la autoría y participación, lugar del hecho y responsabilidad, entre otros, que se tengan en actos ilícitos dentro de una empresa, ya que sin ello no existe una posibilidad de confrontar a nuevas formas de delitos cibernéticos. Al tener este problema y ver que en los últimos años el cibercrimen puede golpear a los ciudadanos o las empresas individualmente, como lo mostró el estudio *Security Report Latinoamérica 2016, de la firma Eset*, revelaba en una investigación regional, que casi un 45% de las empresas costarricenses sufrieron ataques informáticos, es por ello que existe la necesidad de buscar soluciones o medidas que colaboren a mitigar estos ataques, y así mismo responsabilizar también, como lo indica el CEC, a las personas jurídicas, para otorgar verdaderas garantías de protección a los usuarios, y mantener un equilibrio, logrando posicionarse frente a otros países que cuentan con todas las disposiciones legales

para hacerle frente a esta poderosa arma que es la tecnología, y que se encuentra a disposición de las grandes compañías que manejan muchos datos personales y parte del patrimonio económico costarricense.

1.1.2 Problematización del problema

Existe una posición de los tribunales que continúa siendo un problema y se refiere a que los entes colectivos “no tienen capacidad de actuar”, y que solo las personas físicas pueden responder penalmente. Costa Rica tiene un déficit de personal especializado en seguridad informática, así como una débil estructura en oficinas de ciberseguridad dentro de las 342 instituciones públicas del país, en materia legal también existen algunos vacíos, por lo cual, una de las tareas es implementar un plan estratégico de tecnología de la información nacional, que en este momento no existe, así como evaluar alternativas para corregir y mitigar esta tendencia.

Esto ha sido un problema en el sistema jurídico, ya que casi siempre se va un paso atrás en cuanto a la creación de un marco jurídico que permita penalizar a la persona moral, en que el sujeto activo muchas veces se encuentra en puestos de confianza y posee privilegios de acceso a todos los datos de los equipos tecnológicos, también

con respecto al sujeto pasivo, en el que es la persona titular de los datos, siendo indeterminado el sujeto, porque puede ser persona jurídica o física.

Según Francisca H. de Canales en su obra metodología de la investigación año 2007 página 262: “todo hecho anterior a la formulación del problema que sirva para aclarar, juzgar e interpretar el problema planteado, constituye los antecedentes del problema”.

1.1.3. Justificación del Problema

Evaluar la idoneidad de nuevas alternativas como lo es la aplicación de un plan estratégico de tecnología de la información nacional y una efectiva aplicación de la ley sobre conductas ciber delictivas, con verdaderas garantías de protección, dado que factores como la evolución tecnológica, falta de asociaciones entre los sectores público y privado, y la alta vulnerabilidad de las empresas, es un problema importante a nivel país, por lo que la evaluación y análisis de otras alternativas, es clave en la búsqueda de soluciones.

Hay gran relevancia social en el estudio de este tema, ya que Costa Rica se encuentra en la segunda posición de las naciones latinoamericanas que más ataques cibernéticos registra a empresas e instituciones, según el Eset Security Report Latinoamérica 2018, en el que la posición del país hasta este momento, es de alta vulnerabilidad, y más cuando el delito informático es trasnacional, se patentiza la necesaria aprobación de un tratado internacional que unifique criterios,

tanto sustanciales como procesales, y establezca las pautas por seguir en tema de cooperación judicial internacional, de lo contrario, será imposible disminuir los altos índices de impunidad registrados en esta materia.

Debido a lo anterior, ha sido casi imposible conocer la verdadera magnitud de estas faltas, ya que la mayor parte de ellos no son descubiertos, o no son denunciados ante las autoridades, debido a la ausencia de medidas preventivas , a esto hay que sumarle la falta de una apropiada legislación que ampare a las víctimas como ya pasa en otros países, así mismo la falta de preparación por parte de los funcionarios que administran la justicia en Costa Rica, para entender, investigar y aplicar el tratamiento jurídico adecuado para esta problemática. También existe un temor por parte de las empresas y las consecuentes pérdidas económicas, entre otros más que estas pueden tener al regularse la persona jurídica en el ámbito penal, debido a que muchas de las denuncias se darían a conocer en este ámbito y afectarían la imagen de la empresa, pero a su vez, brindaría seguridad a la población en general, fortaleciendo las políticas de seguridad que estas deben tener una vez que se integre el articulo 12 sobre la “Responsabilidad de las personas Jurídicas” del Convenio con Europa que los legisladores costarricenses descartaron.

Según Roberto Hernández Sampieri, en su obra metodología de la investigación 2014, sexta edición en la página 41: “La justificación de la investigación indica el

porqué de la investigación, exponiendo sus razones. Por medio de la justificación, se debe demostrar que el estudio es necesario e importante”.

1.2 FORMULACIÓN DEL PROBLEMA

¿Es idónea la aplicación de una legislación en el país que castigue a las personas jurídicas de la forma como lo desease el convenio?

¿Se deben adaptar penas interdictivas a las personas jurídicas en las que se declare responsable de ello, no solo por los actos de sus empleados en los ciberdelitos, sino también por los de sus administradores o representantes?

1.3 OBJETIVOS

Según Roberto Hernández Sampieri: en su obra metodología de la investigación 2014, sexta edición en la página 37” Los objetivos de la investigación, tienen la finalidad de señalar a lo que se aspira en la investigación y deben expresarse con claridad, pues son las guías de estudio.”

1.3.1 Objetivo General

Según César Augusto Bernal en su obra metodología de la investigación para administración, economía, humanidades y ciencias sociales año 2010 página 99:” El objetivo general debe reflejar la esencia del planteamiento del problema y la idea expresada en el título del proyecto de investigación”.

Se determina el siguiente objetivo general:

Determinar jurídicamente la idoneidad de la aplicación de una regulación adecuada contra la ciberdelincuencia, mediante la adopción legislativa del CEC que responsabilice a las personas jurídicas mediante penas interdictivas en Costa Rica.

1.3.2 Objetivos Específicos

Según Álvarez (2015) en su obra Guía metodológica para la elaboración de proyectos de investigación en postgrado. Los objetivos específicos "indican lo que se pretende realizar en cada una de las etapas de la investigación. Estos deben ser evaluados en cada paso para conocer los distintos niveles de resultados."

1. **Analizar las consecuencias y la importancia de incluir medidas preventivas de las actividades operativas informáticas, de la posesión de la información y del poder de decisión de los órganos directores dentro del sector empresarial, creando un cambio de conciencia de la necesidad urgente de contar con las herramientas necesarias en Costa Rica.**

2. **Indagar, dentro de la legislación costarricense, la viabilidad jurídica que permita desarrollar una adecuada integración de normas mediante la base de legislación comparada en la que se apliquen penas a las personas jurídicas en casos de delitos informáticos.**

3. **Otorgar los elementos de información necesarios, para lograr una percepción social conveniente, a fin de poder desarrollar una política de seguridad informática debido a la alta vulnerabilidad de las empresas en Costa Rica.**

4. **Analizar el concepto de delitos informáticos en las personas jurídicas, y su evolución histórica.**

1.4 ALCANCES Y LÍMITES DEL PROBLEMA

Alcances

Esta investigación debe servir como base de referencia para otros estudiantes y profesionales que tengan un interés por el tema y puedan tener una guía de introducción e información, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juegan las personas jurídicas ante este tipo de hechos.

La investigación abarca el desarrollo de las medidas necesarias para garantizar que se pueda exigir la responsabilidad de las personas jurídica en los juzgados de Costa

Rica, no solo por los actos de sus administradores o representantes, sino también por los de sus empleados, ya que cumplir con el artículo 12 del CEC, daría al país un instrumento importante en la lucha contra el cibercrimen, y al movilizar la ayuda mutua entre los países que integran el Convenio para afrontar delitos informáticos, en vista de su gran complejidad que en muchos casos reviste este tipo de actos tecnológicos, al poder tornarse en una gran cantidad en delitos transfronterizos, además del análisis de otras legislaciones internacionales que pertenecen al CEC relacionadas con el castigo y medidas que han tomado para penalizar a la persona jurídica, debido a la alta vulnerabilidad que sufren las empresas costarricenses, y a la falta de mecanismos legales que impulsen un adecuado sistema de seguridad, en el que los usuarios sientan confianza de los sistemas electrónicos que se manejan de manera externa e interna, esto se llevará a cabo durante el 2019, lo cual beneficiaría a las instituciones, empresas y a la población en general, así como al sistema judicial del país.

Limitaciones

Se poseen limitaciones en cuanto que el sistema penal costarricense está basado en la imputabilidad personal o subjetiva, en la que necesariamente se debe demostrar la participación personal del imputado en los hechos objeto del proceso, para posibilitar la imposición de una sanción de naturaleza penal, además, resulta un problema central la dispersión de las actividades operativas, de la posesión de la información y del poder de decisión que tienen las empresas en el país.

Otra limitante es que la mayoría de las empresas en el país, no poseen un sistema de detección y prevención de delitos en el seno de la organización empresarial, debido a las afectaciones económicas que pueden sufrir si se incluyeran este tipo de políticas y penas en el país, lo que viene denominándose en el ámbito anglosajón como corporate compliance, y que a nivel global, las personas jurídicas lo están utilizando como parte de las nuevas políticas de seguridad, para evitar penas interdictivas incorporadas en sus legislaciones, lo cual, debido a la falta de conocimiento de los legisladores y jueces de la República, ha sido difícil poder hacerle frente a nuevas formas de crimen cibernético.

CAPÍTULO II

MARCO METODOLÓGICO

2.1 TIPO DE INVESTIGACIÓN

Según Finol y Camacho (2008, p.60), el marco metodológico está referido al "cómo se realizará la investigación, muestra el tipo y diseño de la investigación, población, muestra, técnicas e instrumentos para la recolección de datos, validez y confiabilidad y las técnicas para el análisis de datos".

Finalidad: en el presente trabajo el tipo de investigación es teórica, ya que tiene la finalidad de adquirir nuevos conocimientos que permitan solucionar la impunidad que tienen las personas jurídicas en Costa Rica sobre los cyberdelitos, proponiendo la aplicación de penas interdictivas así como el cumplimiento de políticas de seguridad a nivel empresarial que sean debidamente supervisadas.

Dimensión temporal: este estudio tiene una dimensión temporal longitudinal, ya que recolecta datos de otras legislaciones internacionales adheridas al CEC y analiza su desarrollo, en diversos momentos y a lo largo del tiempo, para evaluar su capacidad en la aplicación del marco legal penal en Costa Rica.

Carácter: Esta investigación es de tipo exploratoria ya que la aplicación de penas interdictivas para las personas jurídicas que cometan delitos informáticos en el país, no se han establecido ni planteado, por lo que se busca investigar a fondo y familiarizarse con nuevas tendencias globales que señalen por qué Costa Rica debe incluir de forma estricta en su marco legal, este tipo de actos.

2.2 SUJETOS Y FUENTES DE INVESTIGACIÓN

2.2.1 Sujetos de información

El análisis de los sujetos cumple una función activa en el proceso para toda investigación, ya que son esenciales para el conocimiento y recolección de información necesaria que busca, como objetivo de la investigación, encontrar opiniones importantes en el tema de seguridad electrónica en las empresas del país y la falta de regulación adecuada hacia los delitos informáticos cometidos por las personas jurídicas.

Según Levin & Rubin (1999), una población “es el conjunto de todos los elementos que se estudian y acerca de los cuales se intenta sacar conclusiones” (p. 135).

En esta investigación, los sujetos de estudio van a ser las posibles víctimas, como lo son los usuarios, así como empresarios o representantes de personerías jurídicas y abogados en temas relacionados con el derecho informático, civil y penal.

2.2.2 Fuentes de información

Las fuentes de información son todos aquellos documentos que de alguna u otra manera difunden los conocimientos de un área, tales como: administración, política, educación, salud, derecho. Al llevar a cabo la investigación, se deben manejar fuentes de información que sirvan de base para desarrollar el trabajo de campo.

De acuerdo con Santesmases (2009) La fuente de información, es la persona, organización u objeto de los que se obtienen datos para ser analizados; El dato es el valor de una variable o de una constante, proporciona información sobre una situación y sirve de base para el análisis estadístico; los datos pueden ser primarios o secundarios de acuerdo (sic) la información de la que procedan (pag.75).

Para este estudio, las fuentes de investigación serán de primera mano, tales como las leyes consultadas, entre ellas están, la Ley No. 9048 de delitos informáticos, legislación comparada, y el Convenio sobre la Ciberdelincuencia de Budapest.

Se consultan como fuentes de información las siguientes tesis:

Autor	Universidad	País	Año
Silvia Jiménez Z. Sofia Sancho V. "*Enfoque Laboral de los Delitos Informáticos en la Empresa Privada"*	Universidad de Costa Rica	Costa Rica	2011
Miguel Polaino N. "*Responsabilidad Penal Por Omisión del Órgano Directivo de la Empresa"*	Universidad de Sevilla	España	2016
Jacinto Perez A." *Sistema de Atribución de Responsabilidad Penal a las Personas Jurídicas"*	Universidad de Murcia	España	2013
Ligia Maribel Garcia J. "La investigación de Delitos Emergentes en Internet, su Detección y Control"	Universidad Rafael Landívar	Guatemala	2014

2.2.3 Fuentes de segunda mano

De acuerdo con Escalona (1998), Las fuentes secundarias son documentos que compilan y reseñan la información publicada en las fuentes primarias. Recuerda que el documento primario es la fuente del dato original; mientras que el secundario lo

retoma, de acuerdo con las funciones que desempeña en el campo del conocimiento.

Por lo cual, se utilizan algunas fuentes como Víctor Jiménez, Hispajuris. Cynthia Solis y Vincent Lemone, La Transposición del Convenio de Budapest sobre la Ciberdelincuencia en La Legislación Francesa en La Práctica. Maria del Roció Ramirez González, Métodos de la investigación. Universidad Hispanoamérica Guía para la confección de los Trabajos Finales de Graduación entre otros.

2.2.4 Fuentes de tercera mano

Según Silverstrini y Vargas (2008) Las fuentes de tercera mano son guías que contienen información sobre las fuentes secundarias.

Dentro de las fuentes de tercera mano están el artículo de El Financiero sobre la oficina que vela por la ciberseguridad en Costa Rica de Krissia Chacón en el 2018, el artículo de Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo de Jesús Alberto Loredo González en el 2013, el artículo del Poder Judicial de Costa Rica, Ciberdelincuencia: Delitos sin Fronteras hecho por Andrea Marín Mena en el 2012, entre otros.

2.3 TÉCNICAS E INSTRUMENTOS PARA RECOLECTAR INFORMACIÓN

2.3.1 Método Entrevista

Según Folgueiras (2009) “Técnica orientada a obtener información de forma oral y personalizada sobre acontecimientos vividos y aspectos subjetivos de los informantes en relación a (sic) la situación que se está estudiando”.

El método que se utilizó fue la entrevista, mediante la cual se realizó una serie de preguntas al entrevistado vía video conferencia Skype por parte del entrevistador, en este caso, el entrevistado es el Licenciado José Adalid Medrano, especialista en derecho informático coredactor de las recientes reformas al Código Penal Costarricense sobre delitos informáticos (9048 y 9035), determinando las variables e indicadores para responder en parte a los objetivos específicos estipulados en esta investigación.

2.3.2 Instrumento

Según Rodriguez, Gil y Garcia (1996) “este instrumento se asocia a enfoques y diseños de investigación típicamente cuantitativos, porque se construye para

contrastar puntos de vista, favorece el acercamiento a formas de conocimiento nomotético no ideográfico, su análisis se apoya en el uso de estadísticas que pretenden acercar los resultados en unos pocos elementos (muestra) a un punto de referencia más amplio y definitorio (población) y, en definitiva, porque suelen diseñarse y analizarse sin contar con otras perspectivas que aquella que refleja el punto de vista del investigador".

El instrumento que se utiliza para la entrevista es el cuestionario, el cual consta de una serie de preguntas que se le aplican al encuestado, para que así se generen los resultados de las variables que se van a determinar por parte de este instrumento, que se estructuró con preguntas abiertas y cerradas, dirigidas al sujeto de estudio.

CAPÍTULO III

DESARROLLO

3.1 ESCASA EVOLUCIÓN TÉCNICO JURÍDICA DE LOS CIBERDELITOS EN COSTA RICA

El desconocimiento que se posee entre los usuarios que acceden a muchos de los servicios que son brindados por empresas en el país, facilita el ser víctima de la ciberdelincuencia y para esto es importante que primero se cuente con un conocimiento básico de lo que es un delito informático, tal como lo define el abogado e ingeniero informático, Lic. Roberto Lemaitre “Delito informático es aquella acción típica, antijurídica y culpable realizada por medios informáticos o cuya acción por modificar los datos a un dispositivo”, el cual puede ser realizado por una persona, grupo de personas o un órgano director que maneje información sensible y privada.

Para tener un poco más claro cómo se da usualmente este tipo de delitos mediante los sistemas informáticos, se debe conocer su proceso que consta de tres etapas: el ingreso, el procedimiento y la salida de información, y del cual el 85% de los ataques cibernéticos ocurren en la primera fase, en la que se analiza y se identifica el objetivo para encontrar una manera de acceder a la información, esto ocurre ya sea que se trate obtener accesos a información muy privilegiada, o también mediante personas que ya lo poseen a lo interno, y que muchas veces de manera regular, cuentan con información personal y financiera de los clientes.

Según la Organización de Naciones Unidas (ONU), la creciente conectividad y la gran cantidad de información personal y empresarial, también atrajo a una gran cantidad de delincuentes que buscan sacar provecho de los descuidos de las personas y de las empresas. En este momento, de acuerdo con el organismo internacional, los delitos cibernéticos afectan a unos 431 millones de personas en todo el mundo.

A veces, tanto empresas del sector privado como público del país, deben saber lo necesario, crítico y delicado que es hoy en día este tema, del cual deberían manejar una política que cumpla con los lineamientos más altos de seguridad, que sean estipulados por ley para la protección de la ciudadanía en general como la de sus empleados. Por eso es importante que todos conozcan el impacto de las nuevas tecnologías en el ámbito social y empresarial y que exista una actualización constante de la legislación tal y como lo hace la tecnología.

Los vacíos que aún se encuentran en la legislación costarricense en materia de ciberdelitos, son producto del constante avance tecnológico que ocurre día con día de manera global, para los que contemplan solamente sanciones a personas físicas y no a las personas jurídicas que comentan actos ilícitos, con lo que se facilita el crimen organizado y la continua impunidad a muchos de sus infractores que realizan este tipo de actos, debido también al temor de desprestigio en su imagen como empresa y de sufrir pérdidas millonarias, por eso se requiere de un trabajo

dogmático que incluya juristas, estudiantes, población y empresarios a nivel nacional y conozcan la trascendencia de este tipo de delitos.

3.1.1 *Softwares* Maliciosos

Se habla de *software*s maliciosos, conocidos también en inglés como “malware”, que está diseñado para acceder a un equipo electrónico, e inclusive afectarlo sin que el usuario sepa de ellos, también de forma física por medio de USB. Entre este tipo de software se encuentran los virus, el robo de información confidencial (*spyware),* gusanos, y códigos que se infiltren.

Parte importante de saber cómo se efectúa el delito, es conocer sobre la intención con el que su creador hizo el software, más que sus características. En la actualidad, la gran mayoría de este tipo de softwares maliciosos, se crean con la intención de extraer dinero como forma del crimen organizado, muchos de ellos integrados por los empleados de las empresas (*insiders),* a quienes se les facilita poder ocultar pruebas delictivas en “paraísos informáticos” o sea en países como el nuestro, donde carece de políticas severas de seguridad informática así como legislación que castigue a estas entidades comerciales o financieras, lo que hace aún más difícil seguirles la pista.

Según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, la gran mayoría de los ciberdelitos fueron realizados por empleados de la propia empresa afectada *(Insiders*). También, otro estudio realizado en América del Norte y Europa indicó que el 73% de las intromisiones informáticas cometidas eran imputables a fuentes interiores y el restante a la práctica delictiva externa (*Outsiders*).

3.1.2 Sabotajes desde el interior de la empresa (*Cracker*)

En muchas ocasiones, existen dentro de las empresas algunos empleados que poseen un tipo de conducta poco profesional, que algunas veces desean sabotear a la misma empresa, o a alguno de sus compañeros, pero a veces, de igual forma, ocurre con altos jerarcas en condición de asociados ,accionistas de una personería jurídica, del cual tienen acceso para modificar sistemas de información y datos, o inclusive dar la orden para que otros de rango menor las ejecuten en su lugar, con lo que afectan muchas veces el patrimonio de la empresa, así como a una gran cantidad de usuarios que se convierten en los sujetos pasivos de la cadena alimenticia de estas actividades informáticas delictivas.

Derivado del *hacking* que más adelante se explicará, se encuentra el *cracker* que como anteriormente se explicó, usualmente actúa sin ningún derecho a sabotear

sistemas informáticos, con el fin robar, modificar o destruir información sumamente valiosa para la empresa, hasta al punto de realizar transacciones de forma ilícita.

3.1.3 Intromisión y modificación en base de datos.

Lo que se pretende con este tipo de delito dentro de las empresas y comercios, es obtener información crítica de los usuarios o inclusive desviarla hacia otro punto que no sea el destinado, para poder observar datos o archivos y sus contenidos en la red, esto es muy común en los bancos y casa de bolsas o lugares donde los usuarios manejen constantes flujos de información monetaria.

Este tipo de ataques se dan cuando existe algún tipo de vulnerabilidad en los sistemas informáticos a lo interno y cuando muchas veces ni existen protocolos de seguridad ni escaneos constantes a las herramientas electrónicas que usan muchos de los empleados, con lo que se facilita este tipo de actos ante la poca vigilancia, inclusive de sus propios superiores. Se puede citar, entre este tipo de delitos, a las bombas lógicas (*logic bombs*) que lo que pretenden es dañar datos, ordenar pagos o inclusive hacer transferencias electrónicas de dinero, en los que el creador de un código lo hace mediante una condición que no se replica, y usualmente los crean personal interno de la empresa, que muchas veces se detecta mediante un consumo excesivo de recursos del sistema, destrucción de ficheros, salida de información crítica y confidencial.

Cuando se producen este tipo de actos internos, pocas veces salen a la luz, ya que las empresas prefieren no dar información o publicidad del ataque para no desvalorar la imagen dentro del mercado y perder credibilidad en los clientes.

3.1.4 Falsificación de documentos electrónicos

Parte de los errores que se cometieron en las reformas 9048 y 9135 al Código Penal y que aún no se encuentran corregidos en el nuevo proyecto de ley impulsado por el jefe de fracción del PUSC, Erwen Masis sobre delitos informáticos, en el que existe una serie de problemas dentro de la figura tradicional de la falsificación de documentos en el Código Penal. Se deben plantear nuevas regulaciones en el ámbito propiamente de los delitos de falsedad documental consecuencia del art. 7 de la Convención de Budapest, que busca la protección de los documentos electrónicos no solo en lo penal, sino también en el derecho privado, del cual se trata de comprobar de qué manera afectan estos documentos electrónicos en los diferentes ámbitos jurídicos que deberían estar protegidas por un marco legal.

En la actualidad, en Costa Rica, la materialidad es uno de los requisitos del "documento" que se encuentran en los artículos 359 al 362 del Código Penal, donde según el Lic. Juan Bustos Ramirez, es "una concepción muy restringida de los documentos que ya no obedecen a las formas modernas de las relaciones jurídico-sociales", aquí se pueden enumerar tres de los principales problemas en los documentos electrónicos, la materialidad del documento, el concepto de documento en la doctrina, y la manifestación de voluntad en el documento, debido a que mientras no se imprima el documento, no existirá la materialidad del mismo, ni ningún problema para insertarlo en el tipo tradicional.

Hay que entender que muchos fraudes informáticos se realizan por medio de falsificaciones de documentos, operaciones que se ejecutan mediante un programa

manipulado por algún colaborador de la empresa, en el que se pueden insertar o modificar órdenes de entrega, salarios, mandatos, con lo que se crea un dato informático falso.

3.1.5 Propiedad Intelectual Digital

La propiedad intelectual, muchas veces se puede encontrar también en los delitos informáticos ligados a lo interno de la empresa. El administrador de una página web o de una aplicación informática empresarial tiene las herramientas y permisos que son aportados en su mayoría por directrices de alto rango, esto permite el plagio, distribución, o comunicación de contenidos protegidos, puedan llegar a manos del público o a la competencia.

Con la proliferación de nuevas tecnologías, la reproducción ilegal de contenido del autor crece día con día, y algunas veces los mismos jerarcas de las empresas no conocen en manos de quien ponen estas herramientas que poseen *copyright,* y del cual debería existir una continua vigilancia de sus administradores que cuentan con privilegios e información crítica para el desarrollo diario laboral. Es imprescindible que se adopten medidas técnicas, funcionales y organizativas para proteger los intereses de los usuarios y las empresas, respetando los derechos que posee el autor que desarrolló el programa para poder garantizar el uso correcto, mediante la adecuación de una correcta normativa en el derecho informático que permita proteger los datos.

Como bien se sabe, el bien jurídico que se buscaría proteger con una integración al marco legal costarricense, son los aspectos patrimoniales que los derechos de autor protegen en los programas informáticos, ya que son fundamentales para la sociedad, debido que si no se respetan, no se puede contar con un correcto funcionamiento del mercado. Claro ejemplo de esto es cuando se da la piratería informática, que muchas veces es concientizada por sus mismos administradores o representantes legales de una empresa, al reproducir material ilegal de fuentes o aplicaciones de *software,* tal como los de Adobe para su utilización interna, la distribución de versiones educativas como cursos especiales a clientes sin autorización, duplicado de usuarios con licencia para usuarios sin licencia, o una empresa que oculta el número real de equipos en los que se utiliza un programa, todos estos tipo de delitos de propiedad intelectual deben adecuarse a la legislación y conocerse, a fin de que se tenga un mejor conocimiento de las herramientas informáticas que se usan y el correcto trato y vigilancia que deben darle sus empresarios.

3.1.6 Espionaje Informático Comercial

Otro error cometido durante la implementación de los tipos penales sobre delitos informáticos durante la reforma al Código penal, fue al tipificar los actos de espionaje ya que estos son variados en la red.

Cuando se ingresa a un sistema informático con una clave escaneada o falsa, podría sancionarse como un acceso ilegal o no autorizado, pero entonces es cuando se debe s hacer la diferencia que existe en ambas figuras en cuanto al dolo, la primera podría significar simplemente el acceso no autorizado con una clave falsa mientras que en el espionaje informático implica una intención, la de apropiarse de secretos industriales y comerciales, como ocurre actualmente, no solo como lo describe el articulo 288 en la reforma N° 9048, que deja una muy limitada interpretación con vacíos legales, que no sustentan una realidad global en el mundo de la era digital y empresarial.

"***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."

Costa Rica no posee una figura relacionada con este tipo de acción delictiva, es claro que la reforma contiene el delito de espionaje, pero no sobre el problema planteado, acerca del que no se podría sancionar, la sustracción de secretos de una empresa por un particular, o conjunta con otros sujetos de igual condición jurídica.

Aunado a lo anterior y con el efecto de agravar la existencia de este tipo de vacíos, en Costa Rica no existen mecanismo de *ciber security* que sirvan para prevenir o sancionar conductas lesivas, legalmente constituidas mediante mecanismos digitales.

Este tipo de acciones vulneran los proyectos de las empresas y van directamente relacionados con la revelación de secretos la que en su mayoría es utilizada en beneficio de terceros, como puede ser su competencia u otros sujetos, para obtener una ventaja en el mercado, y así llevan a muchas hasta perder competitividad, clientes, posicionamiento en el mercado y el avance en proyectos de gran impacto para la sociedad.

Según José María Alonso, Director Operativo de Zenit Detectives: “Los perfiles de empleados que realizan espionaje industrial son muy variados. En los casos que hemos investigado hemos encontrado desde trabajadores descontentos, hasta secretarias o directivos”.

Cabe recalcar nuevamente, que dentro de este tipo de investigaciones relacionadas por profesionales, salta a la luz la mano delictiva conformada por directivos de alto rango, quienes muchas veces dan una orden a sabiendas que poseen una armadura de impunidad ante este tipo de ciberdelincuencia, que no se encuentra claramente tipificada, y a su vez, como ya se ha hablado anteriormente, aún no existen sanciones para las personas jurídicas, de las que muchos de estos directivos forman parte.

3.2 RESPONSABILIDAD DE LAS PERSONAS JURÍDICAS EN EL SENO DEL ORDENAMIENTO JURÍDICO COSTARRICENSE.

En Costa Rica, aún no es posible atribuir responsabilidad penal a las personas jurídicas (societas delinquere non potest), la capacidad de acción, culpabilidad y de pena, demanda la presencia de una voluntad, ya que esta actúa a través de la persona individual, que no existe en la persona jurídica. Pero la corrupción y las acciones del crimen organizado, lo han utilizado a su favor en las formas que estas pueden delinquir, esto no quiere decir que el derecho deba permanecer pasivo ante los abusos constantes que estas comenten, especialmente en el ámbito económico, sobre todo en las sociedades anónimas, deberá existir una discusión doctrinal para atribuir la responsabilidad penal a las personas jurídicas por la comisión de delitos informáticos, tal y como lo establece la Convención de Naciones Unidas contra la criminalidad organizada (2000) , el Convenio Penal del Consejo de Europa sobre la corrupción (1999) y el Convenio de Budapest (2001).

La *ius puniendi* lo que busca es impedir y sancionar las acciones que perturben la convivencia social, que quebranten los derechos de los ciudadanos, como ya se sabe, la facultad punitiva procede de la soberanía del Estado, porque tiene bajo su protección el hacer lo mejor posible para el desarrollo de la vida social, está obligado a impedir que se dé la realización de hechos que altere este equilibrio dentro de la sociedad. En la comisión de la conducta punible, se suele encontrar dos sujetos,

uno activo, que en la mayor parte es una persona individual que podría asociarse con otras personas, y que realiza de manera directa o interpuesta la conducta antijurídica, y el sujeto pasivo que puede ser una persona natural o moral, o un ente colectivo titular del bien vulnerado. Es conocido que las personas jurídicas tiene capacidad de acción, tales como: celebrar acuerdos, contratar, fabricar y desarrollar actividades económicas etc., y del cual existe un punto de referencia para dar la existencia a una posibilidad de adjudicar responsabilidad penal a las personas jurídicas que comentan delitos informáticos, que se ha ido aceptando en América Latina, Venezuela y en Chile, que proviene del modelo de las naciones del Commonwealth, allí se refuerza el argumento que a través de la conducta manifiesta de los integrantes de las personas jurídicas, las hace tener una identidad absoluta, y por ende, ese comportamiento punible ejecutado por sus órganos de dirección, puede ser atribuido al ente colectivo, indicando que detrás de ella hay personas naturales que son responsables de las conductas de la organización.

Para fundamentar la posibilidad de atribuirles una responsabilidad por ciberdelincuencia a las personas jurídicas se hará referencia a modelos como el de la identidad, que señala que al igual que una persona física, la persona jurídica cuenta con una cabeza que toma las decisiones y unos órganos que la ejecutan, esta tesis es aceptada en diferentes sistemas y en leyes específicas, como la que sanciona el homicidio culposo cometido por fabricantes de vehículos automotores en Inglaterra, también se encuentra, en el sistema norteamericano, el modelo vicarial, que traslada automáticamente a la persona jurídica la responsabilidad

penal derivada de una acción cometida por una persona física que la compromete, siempre y cuando exista una conexión.

Se deben tomar en cuenta estas nuevas formas de enjuiciamiento, ya que la culpabilidad del ente colectivo debería manejarse con base en la premisa de que su actividad y su representación son manejadas por personas naturales, por lo que el legislador, de acuerdo con el principio de legalidad, puede establecer conductas que se consideren delictivas y establecer sus penas.

Según Bacigalupo (2001, pág. 369) “para determinar cuáles son las personas dentro de la estructura de una sociedad que tienen capacidad para representarla jurídicamente, se debe recurrir a la ley o al estatuto social. De esta manera, se debe considerar con capacidad de representación y, por lo tanto, con capacidad de dar lugar a responsabilidad penal las acciones llevadas a cabo por un órgano o un miembro del órgano de representación de las personas jurídicas”.

Una buena alternativa para incorporarla a la legislación costarricense, es que todo aquel que actúe como directivo en representación del ente colectivo, de una manera voluntaria o delegada, debería responder por cualquier acto informático delictivo que se cometa, con lo que se abre la posibilidad real, tanto a la persona física como la de la jurídica en el país.

Según afirma Garcia Cavero (2005 pág. 135) “No hay duda de que la empresa ha desplazado a la figura del comerciante individual en el terreno de la economía, lo que explica no sólo que la normativa jurídico-privada haya tenido en cuenta desde hace tiempo el fenómeno corporativo en la constitución de las relaciones jurídicas, sino también que el propio sistema penal comience a plantearse en la actualidad la necesidad de considerar a la persona jurídica en sus criterios de imputación de responsabilidad.”

3.2.1 Deberes y Responsabilidades de los Directores, Administradores o Representantes Legales en las Personas Jurídica.

Hoy en días se ha visto como la proliferación de las personas jurídicas dentro de la industria, es una realidad, en él se encuentra, desde la custodia de activos hasta el desarrollo y operaciones de negocio, aun así, se suele pasar por alto las responsabilidades relacionadas con estos puestos, que poseen un gran poder de representación ante terceros, como miembros de un órgano director y representantes legales.

Se supone que los directores, consejeros, administradores tienen un deber de lealtad y cuidado a la hora de actuar, haciéndolo siempre de buena fe, para beneficio de la persona jurídica y sus intereses. El código de comercio deja claro las responsabilidades y obligaciones que estas personas poseen, así como sus eximentes, formas de extinción y las formalidades para exigirlas.

En Costa Rica, existe la responsabilidad del director si este ha producido un daño, también responderán solidariamente todos los miembros del órgano, a menos que alguno de sus miembros pruebe que no sabía de la existencia de tal acto, que en caso de saberlo haya realizado todo lo posible para impedirlo, reduciendo inclusive las consecuencias de no haberlo impedido parcialmente. Es importante abordar lo relevante que es el poder de mando y conducción que poseen cada uno de estos puestos, ya que gran parte de estos ciber delitos se gestan en el seno de una corporación, en especial de las grandes trasnacionales, las cuales en Costa Rica poseen mucho poder económico, y en tal sentido, las personas jurídicas son utilizadas como un instrumento ideal para cometer actividades ilícitas de negocios.

En ocasiones, por medio de sus administradores o representantes legales, pueden servir como mediadores de la acción delictiva, mediante el uso de mando pueden ejecutar órdenes contrarias a la voluntad del órgano directivo o la sociedad, a sabiendas de que no poseen muchas veces una adecuada vigilancia de sus actos, y que mediante agentes de soporte técnico, contadores, *managers*, entre otros hagan posible actos que provoquen en el ciberespacio un perjuicio grave a los consumidores o usuarios de la red, con tal de obtener beneficios en el mercado.

En las sociedades puede existir las responsabilidad administrativa, civil, penal, administrativa, y laboral, o inclusive varias de ellas, como pasa con las penas

interdictivas que van desde la pérdida de patente, cierre de negocios, disolución de la sociedad, no poder realizar negocios ni contratos etc.

La responsabilidad corre en manos de quienes tomaron la decisión o de quienes la ejecutaron, El Código de Comercio establece en los casos de responsabilidad, un régimen a lo interno y a lo externo, del cual del primero es la Junta para con la Asamblea de socios, los que pueden reclamar o investigar si existen estos actos, a lo externo, existe una responsabilidad de la persona jurídica para con cualquiera. En empresas muy grandes, la junta directiva no abarca el desarrollo de todas las actividades de administración, para esto delega a sus órganos que están representados por apoderados generales, a sabiendas que la responsabilidad sigue siendo de ambos.

La responsabilidad civil que existe en los administradores de las personas jurídicas, se pueden encontrar en dos teorías, una llamada la teoría del órgano y la otra teoría de la representación. En la primera, quien actúa a lo interno y ante terceros en una sociedad, es la persona jurídica como tal, lo cual constituye una unidad indivisible, para la que cualquier acción del órgano de administración es imputable.

En la teoría de la representación, se considera que la persona jurídica actúa por medio de representantes, por lo que cualquier acción que realizan, son imputables a los administradores en forma individual.

En Costa Rica se establece que la administración de la Sociedad la ejerce la junta directiva y la responsabilidad de ella pasa por el administrador o administradores a través del mandato. Hay que recordar que para poder cumplir con esta función, el órgano lo debe dotar de poderes y ámbitos que abarcan aspectos financieros, técnicos y otros tales como delegarle funciones al director financiero, de recursos humanos, de *marketing*, de IT; una delegación que puede basarse en el apoderamiento de tales directivos dándoles responsabilidades de control y manejo de áreas o departamentos, bajo la supervisión directa del administrador. En todo caso, corresponde al administrador el control y la adecuada vigilancia del apropiado desarrollo de todas las decisiones de administración y gerencia. La responsabilidad civil irá dirigida a resarcir los daños patrimoniales que su actuación incorrecta le pueda causar a la sociedad o a terceros, en la relación de daños causados por ser contrarios a la ley o a los estatutos; pero también puede surgir por los perjuicios derivados de los actos realizados sin la debida diligencia correspondiente a su cargo, por lo tanto, debe probarse la acción u omisión gravemente culposa y demostrarse el daño y su relación de causalidad con aquella (nexo causal).

La responsabilidad de los administradores es solidaria. Solo se le puede evitar si se ha votado en contra de un acuerdo y se ha hecho constar así en las actas. Cuando un Gerente o la Junta Directiva actúan extralimitando sus funciones u omitiendo las mismas, ocasionan perjuicios dolosos o por culpa a la sociedad, a los socios o a terceros, el máximo órgano social, que es la Asamblea de Accionistas, tiene la autoridad de iniciar acciones legales contra los administradores irresponsables,

para que respondan solidaria y de forma ilimitada por los perjuicios cometidos de tales actos, que se conocen como la Acción Social de Responsabilidad.

3.2.2 Sujeto Activo de la Persona Jurídica

En los ciber delitos se encuentra la persona del sujeto activo, como aquella que posee ciertas características que no presentan el denominador común de los delincuentes, ya que algunos poseen habilidades informáticas para el manejo de ciertos programase, y usualmente poseen una posición laboral de confianza y privilegio, en lugares estratégicos que controlan información crítica y sensible para poder realizar este tipo de actos delictivos.

Según la tesis de la responsabilidad de Franz Von Lizst y Magiori, ambos sostienen que, si las personas colectivas son capaces de adquirir derechos y contraer obligaciones, también deben responder por los delitos en que incurren como la estafa, el abuso de confianza y entre otros, si bien no se les puede aplicar sanciones privativas de libertad, son susceptibles de sufrir sanciones pecuniarias, y además, las penas corporales se impondrán a sus directivos responsables.

El sujeto activo en los ciber delitos consiste en la influencia de los procedimientos o resultados que este pueda ocasionar en los datos de los sistemas, por medio de

ciertas conductas que incidan, manipulen, alteren la realización de instrucciones de un programa informático. Por ejemplo, en el proceso de pago a los proveedores de la empresa, usualmente existen varios procesos por seguir dentro del sistema, del cual, si alguno se altera fraudulentamente, tendrá efectos negativos en el resto del proceso en el que terceros se afectarán.

Hoy en día, la ley muchas veces debe ir de la mano con los avances tecnológicos, de los cuales requieren una respuesta jurídicamente diligente, para darle un enfoque preventivo a este tipo de situaciones. Con el auge de la internet, muchos programas son puestos a disposición del público en la misma red, lo cual ha permitido una distinción de los sujetos activos por su grado de conocimiento y en el área en que actúan. Por la diversidad de puestos en las empresas grandes, y las diferentes áreas de departamentos que estas poseen, han surgido nuevas formas informáticas de delinquir y que se han clasificado de la siguiente manera:

Phreaker:

Es aquel que posee conocimientos profundos en sistemas de telefonía, tanto terrestres como móviles, *softphones y hardphones* mejor conocidos como teléfonos IP. Estos buscan infiltrar la protección de las redes públicas y corporativas de telefonía que se manejan desde sistemas electrónicos de computación. También, usualmente, operan dentro de las compañías de telefonía y *call centers*, donde adquieren un código identificador del usuario que no les pertenece y cargando el costo de la llamada a la cuenta de la víctima, otro modo operandi es el *diversiting,* el cual penetran de forma ilícita centrales telefónicas privadas que en ocasiones el

propósito es adquirir información importante de algún usuario, y usualmente se da en empresas que tenga un gran volumen de llamadas lo que dificulta más su detección.

Lammers:

Son aquellos que se benefician o aprovechan de un conocimiento adquirido y publicado por expertos, pero su capacidad es muy limitada para poder ingresar a sistemas, mucho joven de hoy en día se encuentra en esta categoría, debido a la gran posibilidad que tienen muchos en entrar a otros sistemas o computadoras de usuarios mediante herramientas de servicio que la misma compañía les ofrece para brindar soporte.

Hackers:

Son individuos con conocimientos avanzados de computación, disfrutan navegar y explorar sistemas informáticos y ampliar sus capacidades, usualmente se encuentran en empresas informáticas. Para los grandes fabricantes de sistemas informáticos este es el grupo más rebelde de todos, ya que usualmente encuentran la manera de irrumpir en sistemas de seguridad donde trabajan, y que muchas veces son vulnerables al no poseer los adecuados protocolos de seguridad que toda empresa debería poseer, para el cuido de información interna y del usuario.

Trashing:

Es considerado una de las más recientes formas de delitos informáticos en las empresas, consiste en obtener información secreta y privada mediante basura digital, descartada por empleados internos con el fin de utilizarla por medios informáticos en actividades delictivas, las cuales pueden tener como objetivo muchas veces, el lucro mediante el uso ilegitimo de códigos de sistemas informáticos mediante el análisis de la basura digital recolectada.

3.2.3 Sujeto Pasivo de la Persona Jurídica

El sujeto pasivo en los ciber delitos es siempre la víctima, el propietario del bien jurídico protegido, al que le recae la acción o omisión que realiza el sujeto activo, en este caso, son individuos como los usuarios, instituciones publicas y privadas, que usan sistemas automatizados de información, generalmente conectados unos con otros.

Debido a la falta de políticas de seguridad y leyes que respalden el cumplimiento de estas, es difícil a veces conocer los tipos de delitos informáticos que se cometen dentro de las empresas, ya que ocasionalmente estos no denuncian a las autoridades para no perder su imagen comercial y de competencia en el mercado, sufrir pérdidas económicas o por la falta de preparación por parte de las autoridades para comprender, investigar y procesar este tipo de actos.

Se debe destacar que los organismos internacionales han adoptado resoluciones similares a las aquí planteadas, en las que mencionan que “educando a la

comunidad de víctimas y estimulando la denuncia de los delitos, se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

3.2.4 Responsabilidad Civil en Materia Informática

El análisis que se hace a continuación, se deduce de una posible aplicación de la disciplina de la responsabilidad civil, contractual y extracontractual, que se da en otras legislaciones que sirven como base para esta investigación, como instrumento en la lucha del ámbito jurídico, donde se desea atender, en las personas jurídicas, la problemática que existe en Costa Rica, de la continua impunidad que prevalece de forma manifiesta en los delitos informáticos a los que se debe dar una solución a temas legales surgidos en un tiempo donde la informática y la tecnología, aún no existían en el país, como ahora, ni muchos en el área de la delincuencia.

Las relaciones que hoy en día se encuentran entre el Derecho y la Informática, son muy complejas y variadas, pero a su vez, no se ha abierto un campo para el estudio y seguimiento de nuevas formas de análisis jurídico que permitan un avance progresivo para la sociedad y brindar una seguridad que claramente es necesaria en los avances tecnológicos que se dan hoy día, en cuestiones tales como: la protección de datos, relaciones contractuales, propiedad intelectual, delitos informáticos y otros. Esto hace que se den cambios estructurales a la hora de abordar estos temas y que de paso exigen mayor control y proteccionismo a las personas que requieren de estos servicios tecnológicos, para las que a veces el

Derecho no puede resolverlas tan fácilmente, de acuerdo con los métodos tradicionales.

Toda actividad que genere un riesgo, es susceptible de producir un daño y, por ende, debe contar con la obligación de responder si este se produjera. Las doctrinas más modernas en el mundo como en España, enseñan que la idea de responsabilidad en estos días se identifica con la de tener que cumplir con compartir las consecuencias de una obligación, Entonces aparecen nuevos principios en este campo de la tecnología y el Derecho para las que han perdido peso elementos tales como la culpa, la casualidad, etc. En estos países se ha afirmado que ya no hay que reparar porque existió una conducta reprobable sino lo que se busca es reparar a secas, asegurando la indemnización a las víctimas en lo que realmente se encuentra el verdadero imperativo social.

Ahora esto no debe llevar a consecuencias extremas ya que acentuar las responsabilidades o la severidad de estos principios, llevaría a que ningún empresario quisiera realizar actividades que tenga alguna especie de riesgo como el de manejar patrimonios importantes de dinero o sobre algunos tipos de información crítica para las operaciones informáticas y operativas de la empresa.

En esta materia, la responsabilidad civil podría atender y ser aplicable dependiendo de las circunstancias de cada caso, por ejemplo, si se desarrollaron contratos relativos a productos informáticos o de servicios, en los que los daños fueron originados en el contenido prestacional de un contrato, pero en tanto el daño provenga del incumplimiento del deber de conducta diligente, sin un contrato de por medio, se estaría ante una responsabilidad extracontractual.

La Sala Primera dice que “la responsabilidad civil extracontractual recae sobre quien, aparte de toda relación contractual previa, causa un daño en la esfera jurídica de otra persona, ya sea por culpa o por medio de la puesta en marcha de una actividad riesgosa o creación de un riesgo social. Esta responsabilidad no nace del incumplimiento de un determinado vínculo, sino de la simple violación del deber civil general de no dañar a otros”. Este régimen está basado en los artículos 1045, 1046, 1047, 1048 del Código Civil costarricense. Es aquí donde el carácter objetivo o subjetivo indicarán el tipo de obligación o responsabilidad que se le debe atribuir al administrador o representante del órgano colectivo, o inclusive, a cada uno de ellos en la medida que hayan intervenido en los medios o resultados del ciberdelito. A su vez, cuando la lesión provenga de la intromisión en la privacidad o transmisión de datos sensibles sin consentimiento de la víctima o afectado, la persona jurídica o natural deberán responder por los hechos causados por su empleados, debido a las normas de responsabilidad “in eligiendo” que se encuentran en el ordenamiento y que deben ser modificadas para esta materia en estudio.

3.2.5 Deberes Exigibles a la Persona Jurídica en el Ámbito Informático

En las empresas se debe tener claro los deberes de conducta exigibles a todo colaborador que tenga algún tipo de relación con los sistemas informáticos y su tratamiento, esto según la función de cada sujeto que desempeñen en esa actividad, del cual serán exigibles deberes en mayor o menor grado. Aquí es donde la persona

jurídica y los actuales criterios de imputación, recomiendan que el titular debe responder por esos deberes y sujetos, salvo exoneración legalmente prevista y que esté debidamente probada.

Tales deberes deben ser, para empezar, en el área de la seguridad, donde el contenido de información debe ser sometido a estrictas reglas de seguridad lógicas y físicas para evitar pérdidas, fugas o usos indebidos prohibidos por Ley, se trata de un deber de diligencia en la gestión y administración por parte de quienes la custodian y manejan esos datos en los sistemas automatizados, por ende, si no se reúnen las condiciones de seguridad necesarias por falta de recursos o debida vigilancia, deberán ser analizados de acuerdo con las medidas preventivas y racionales para evitar una lesión al bien jurídico que se protege.

Seguidamente se encuentra el deber del debido secreto que le impone una conducta a todos los sujetos que, por su relación con estos datos e información crítica de los clientes como de la empresa, deben cuidar no revelar en cualquier fase del proceso y que se extenderá con posterioridad, aunque su relación haya finalizado con las personas titulares de ellos. En la misma línea se da el deber de lealtad, derivado de la buena fe que va ligado al funcionario o colaborador con el titular de los datos, en este caso la empresa o la persona jurídica, ya que después de terminada la relación contractual no puede revelar los datos ni llevárselos para uso persona o de otra empresa, de lo contrario, estaría expuesta a que se le acuse de la comisión de un delito.

En la aplicación de las normas que regulan la responsabilidad civil a la actividad de riesgo que se encuentra en los sistemas de tratamiento automatizado de datos que

este implica, deberán responder penal y civilmente aquellos sujetos en la persona física y jurídica, en la debida reparación de los daños y perjuicios a falta del debido cumplimiento de los deberes que la ley deba indicar.

El deber de información va de acuerdo con la puesta en conocimiento de ciertas circunstancias, cuando se haya afectado a usuarios terceros, entre otros. Y deberán rendir un informe de la afectación con las debidas apreciaciones, evaluaciones de cómo se dio el hecho, cuándo y dónde se originó, y las medidas de seguridad inmediatas que se tomaron para remediar el hecho, o por el contrario, para disminuir el daño ocasionado.

De la misma manera, tienen que existir los deberes de colaboración, los que se obligue a la entidad a cumplir con ciertas directrices de cumplimiento a la hora de que se habra una investigación, por ejemplo, cuando se solicite documentación e información propia del caso para permitir la función inspectora, cuando esta se le exija. Costa Rica debe contar con este tipo de leyes para medir el nivel de diligencia de los titulares y entes colectivos en el desempeño de sus funciones como en otros campos de la responsabilidad civil, en los que existen normas técnicas claramente definidas.

Esta posibilidad abre las puertas a que exista un mejor control legal y a su vez hace que las personas jurídicas y empresarios se ajusten a estas disposiciones legales y reglamentarias, con lo que podrían sufrir multas y penas de no hacerlo, como lo encomendaría una posible ley.

3.3 CONVENCION EUROPEA SOBRE LOS CIBERDELITOS

No es sino hasta en el 2001, cuando se dan las primeras disposiciones emanadas de la Unión Europea, mediante la Convención del 23 de noviembre de 2001 en Budapest. Era necesario que el derecho pudiera darles seguimiento a las evoluciones tecnológicas, además de ofrecer grandes ventajas a la sociedad de hoy en día, así mismo, ofrece un mundo lleno de posibilidades para los delincuentes.

Se sabe que solo un instrumento jurídico internacional puede tener la eficacia necesaria para enfrentar estas nuevas formas de delinquir, y del cual se necesita una cooperación internacional para que con base en los mismos medios informáticos, se permita también combatir esta guerra cibernética. De este convenio la Unión Europea forma parte, sino también los demás Estados firmantes como Costa Rica. Ahora bien, no basta con las buenas intenciones y crear leyes por crear, ya que muchos de los Estados que integran este convenio han tardado demasiado en ratificar y así mismo integrar muchos de sus artículos, lo que ha ocasionado un atraso en sus legislaciones para combatir el cibercrimen, que continúa avanzando de una forma global y apresurada.

Debe existir la necesidad de cooperación entre los Estados, el sector público y privado en la lucha contra la ciberdelincuencia, así como el interés de proteger de forma legítima los bienes jurídicos, para que una lucha efectiva reforzada y eficaz

como lo sugiere este Convenio, ayudará a brindar más seguridad en el desarrollo de los sistemas informáticos.

El presente Convenio fue necesario para prevenir actos en los que se pone en peligro la integridad, seguridad, confidencialidad y la información de datos en las redes de información, garantizando la tipificación de estos contra dichos delitos mencionados en el Convenio, brindando poderes suficientes para una lucha íntegra y facilitar su detección, investigación y penalización, tanto a nivel internacional como nacional, de forma ágil y adecuada, que nazca, como señala su preámbulo, de la necesidad prioritaria de aplicar una política penal común entre sus miembros.

Uno de los problemas es que no todos los Estados parten del mismo contexto, o abordan los mismos problemas, ni poseen los mismos obstáculos, ni tampoco son igual de trasparentes como ya se ha mencionado, no todos los Estados priorizan de la misma manera el respeto a los derechos humanos.

Para este estudio, a partir de la aprobación de este Convenio en Costa Rica, surgen interesantes preguntas en el derecho penal y civil a la hora de analizar una posible responsabilidad a las personas jurídicas, tanto en los casos previstos en la Convención que sean cometidos por cuenta de estas, o por cualquier persona física en su condición de miembro o representante de la persona jurídica.

3.4 DERECHO COMPARADO EN EL DELITO CIBERNÉTICO

Durante las últimas décadas, ha existido en el ámbito internacional un consenso para desarrollar un marco jurídico general de los problemas derivados del mal uso de la informática y de los avances tecnológicos que han dado lugar a nuevas formas delictivas en la mayoría de los países y con especial enfoque en Latinoamérica.

En una primera instancia, en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio en la posibilidad de aplicar y armonizar de manera internacional, leyes penales, a fin de luchar contra el mal uso y de forma indebida de los programas informáticos. Por otra parte, en el ámbito de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), durante el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana, Cuba, se menciona que la delincuencia relacionada con los delitos informáticos era consecuencia del mayor empleo y manejo en los procesos de datos en las economías de muchos países, y que por eso mismo se había difundido a nivel global la comisión de actos delictivos. Por tal motivo, si bien el problema principal hasta ese entonces era el de la difusión y reproducción no autorizada de programas cibernéticos, no se habían difundido otras formas de delitos informáticos, por lo que era necesario desarrollar medidas preventivas para evitar su incremento.

De manera general se supuso que habría un gran número de casos de ciber delitos no registrados, que estos eran un fenómeno nuevo, y debido a la ausencia de

medidas que pudieran contrarrestarlos, se concluyó que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. Debido a esto, el Congreso acordó recomendar que se establecieran normas y directrices sobre seguridad informáticos en los equipos de cómputo, a fin de ayudar a la comunidad internacional a enfrentar estas formas nuevas de delincuencia.

La situación de Latino América, es un tanto curiosa, puesto que con la adopción de modernos códigos de corte acusatorio, han contribuido a que se produzca un cambio en los sistemas procesales en los últimos años, pero que han dejado sin mayores variaciones a los artículos referentes a la prueba, que continúan casi de igual forma que los antiguos.

Es importante siempre recordar la necesidad de una armonización de la que, tiempo atrás, se ha hecho la señalización de que las fronteras nacionales constituyen un obstáculo claro en la detección, análisis, investigación, persecución y castigo de los autores de aquello que han cometido un ciberdelito mediante el uso de nuevas tecnologías de información y comunicación. Las redes de la informática están configuradas con un espacio sin fronteras y para hacerle frente, se tiene claro que la vía más conveniente es con base en el impulso de esfuerzos regionales mediante convenios multilaterales.

3.4.1 Estados Unidos, Primer País en tener una Regulación en el Campo de la Informática.

Es interesante para este trabajo, al menos señalar, sin profundizar mucho, que la primera condena en Estados Unidos se dio por los actos que realizaron daños informáticos sobre sistemas ajenos, lo cual dio el resultado del procedimiento penal del Estado de Texas contra Donald Gene Burleson en 1988, a quien se le condenó por introducir sin autorización, y borrar datos de los ordenadores de la empresa de la que había sido despedido en 1985, la pena fue de siete años de libertad condicional y al pago de 11.800 dólares a la empresa afectada, por responsabilidad civil.

La ley Federal *Counterfeit Access Device and Abuse Act* de 1984 crea un indicador en la regulación penal sobre los delitos informáticos, no solo en los Estados Unidos, sino en el resto del mundo, al ser la primera legislación de carácter nacional que estaba directamente relacionada con este tipo de acciones y que fue promulgada el 12 de octubre de 1984, en la que se establecen diferentes delitos a partir del título "fraude y actividades relacionadas en la conexión entre ordenadores".

Una vez que entró en vigor, se descubrió que como herramienta, era muy importante pero insuficiente ante el avance tecnológico y de los diferentes tipos de actos que iban apareciendo en los ciberdelitos y al no poder ser aplicada a gran parte de ellos.

En la actualidad, Estados Unidos, se destaca por la gran cantidad de agencias y otras instituciones públicas y privadas que se han creado, para dar forma, más allá de los textos legales, de una u otra manera a la protección que la legislación trata

de garantizar. El Instituto de Seguridad en Computadoras (CSI) realiza informes anuales denominados “Estudios de Seguridad y Delitos Informáticos” desde hace más de una década. Así mismo, además de esta organización de carácter privado, se encuentra la institución del Centro de Quejas de Delitos por Internet, por la que existe un gran interés del propio Gobierno estadounidense, y que se autodefine en su web oficial como una entidad gubernamental que establece colaboración con el FBI.

3.4.2 Legislación Comparada en Países de Latinoamérica

Durante la Segunda Reunión de Ministros de Justicia de las Américas, el 1 de marzo de 1999, que tuvo lugar en Lima, Perú, se destacó el tema del delito cibernético como uno de los desafíos con que se enfrentan las Américas. Se reconoció que este tipo de delitos cibernéticos no se limitan a las fronteras políticas y constituye una amenaza para el sistema jurídico y la sociedad. El informe final de esa reunión recomendó a los países de la región hacer un diagnóstico sobre la actividad delictiva vinculada a los sistemas tecnológicos, así mismo un análisis de las legislaciones y prácticas nacionales relacionadas con dicha actividad, e identificar mecanismos de cooperación en el sistema interamericano, para hacerle frente al delito cibernético.

a) **Venezuela**:

En Venezuela, desde el 30 de octubre del 2001, la Asamblea Nacional ratifica la ley especial contra los delitos informáticos. Se observar a continuación, como en su artículo cinco, la sanción contra las personas jurídicas cuando se hayan utilizado medios informáticos para su cometido, es uno de los países con las legislaciones más completas, ya que no solo se encarga de tipificar las distintas conductas delictivas, sino que, a su vez, da conceptos y definiciones para que los artículos puedan ser aplicados eficazmente.

Artículo 5

Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

Después, es importante observar como en esta legislación en los siguientes artículos incluye el agravante especial para las personas jurídicas por delitos cometidos en el artículo cinco antes mencionado; así mismo, las sanciones que

imponen por los actos cometidos en razón del ejercicio de un cargo o función dentro del ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información.

Artículo 27. Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad: 1. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido. 2. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

Artículo 28. Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo cinco de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito. **Artículo 29.** Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente, sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes: 1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos diez y 19 de la presente Ley.

2. El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos seis y ocho de esta Ley.

3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente. 4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30. Divulgación de la sentencia condenatoria. El Tribunal podrá, además, disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31. Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el juez impondrá en la sentencia, una indemnización en favor de la víctima por un monto equivalente al daño causado. Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos.

b) **Bolivia**:

En Bolivia los ciberdelitos son tratados como delitos comunes, están incluidos en el Código Penal y no tienen una ley específica.

c) **Cuba**:

Cuba En la Resolución 204/96, la cual dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y seguridad del Secreto Estatal. Por otro lado, el Decreto Ley 199/99 define como objetivo fundamental establecer y regular el Sistema para la Seguridad y Protección de la Información Oficial. No existe una legislación propiamente para los delitos informáticos, se han localizado diferentes posturas en la doctrina. Se ha dicho que existe una necesidad de una regulación especial en esta materia, pero también debido a la filosofía del Código cubano sobre sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables.

d) Ecuador:

En Ecuador existe la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 2002-67). Lo que buscan con esta ley, es que el Estado Ecuatoriano cuente con las herramientas jurídicas que le permitan un uso debido de los servicios electrónicos, del cual incluyen el comercio electrónico para

adquirir una mayor facilidad de acceso a lo que es cada día más compleja red de los negocios internacionales.

En dicha ley, dentro del Capítulo I del Título V, titulado "De las Infracciones Informáticas", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En él se agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.

e) **Panamá**:

En Panamá se promulgó la Ley No 51 del 2008, la cual regula los documentos y firmas electrónicas además de la prestación de servicios de almacenamiento tecnológico de documentos, certificaciones de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico, de las que aparece un marco regulador en la responsabilidad de los que actúan como intermediarios en estos contenidos por medios informáticos. Se puede observar un régimen sancionador, no solo para las personas naturales, sino también para las personas jurídicas que utilicen estos medios como vemos a continuación.

Artículo 15. Certificados electrónicos de personas jurídicas.

La persona jurídica podrá imponer los límites que considere, por razón de cuantía o materia, para el uso de los datos de creación de firma. Estos límites deberán figurar en el certificado electrónico. Se entenderán realizados por la persona jurídica, los

actos o los contratos en los que su firma se hubiera empleado, dentro de los límites establecidos. Si la firma se utiliza transgrediendo dichos límites, la persona jurídica quedará vinculada frente a terceros, solo si los asume como propios o se hubieran celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona natural responsable de la custodia de los datos de creación de firma, quien podrá repetir en su caso, contra quien los hubiera utilizado.

Artículo 43. Conservación de los documentos electrónicos y archivo de documentos.

El cumplimiento de la obligación de conservar documentos, registros o informaciones en documentos electrónicos se podrá realizar por cuenta propia o a través (sic) de terceros. Toda persona natural o jurídica, nacional o extranjera, que realice almacenamiento tecnológico de documentos de terceros, deberá registrarse ante la Dirección General de Comercio Electrónico, como prestador de servicios de almacenamiento tecnológico de documentos. Las personas jurídicas y naturales que realicen por cuenta propia el almacenamiento tecnológico de documentos, con el interés de que dichos documentos tecnológicamente almacenados tengan el valor legal otorgado por esta Ley, deberán cumplir con los requisitos mínimos establecidos en este Título y en los reglamentos técnicos que emita la Dirección General de Comercio Electrónico. Cuando los documentos contengan datos o información sensible a los intereses de No. 26090 Gaceta Oficial Digital, jueves 24 de julio de 2008 18 19 terceros, quienes realicen el almacenamiento tecnológico de

documentos deberán obtener una aprobación o autorización de dichos terceros, para su conservación.

f) República Dominicana:

En República Dominicana la Ley No 53-07 del 2007 es una Ley Especial contra Crímenes y Delitos de Alta Tecnología. En dicha norma, se regulan algunos principios y conceptos, posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, también posee un capítulo dedicado a la parte procesal penal, así mismo, la propia normativa, genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos. Esta ley es de aplicación general a todas las personas físicas o jurídicas, privadas o públicas, nacionales o extranjeras. Así mismo, hace un desglose de definiciones muy completo, abarcando desde los sistemas y dispositivos informáticos, hasta definir de manera adecuada, quien es el sujetos activo y pasivo hasta el usuario en esta materia.

En el titulo tres de esta ley habla a continuación sobre la responsabilidad Civil y Penal de las Personas Jurídicas, omisiones, acciones administrativas y pagos por indemnización.

Artículo 60.- Responsabilidad Civil y Penal de las Personas Morales. Además de las sanciones que se indican más adelante, las personas morales son responsables civilmente de las infracciones cometidas por sus órganos o representantes. La responsabilidad penal por los hechos e infracciones contenidas

en esta ley, se extiende a quienes ordenen o dispongan de su realización y a los representantes legales de las personas morales que conociendo de la ilicitud del hecho y teniendo la potestad para impedirlo, lo permitan, tomen parte en él, lo faciliten o lo encubran. La responsabilidad penal de las personas morales no excluye la de cualquiera persona física, autor o cómplice de los mismos hechos. Cuando las personas morales sean utilizadas como medios o cubierta para la comisión de un crimen o un delito, o se incurra a través (sic) de ella en una omisión punible, las mismas se sancionarán con una, varias o todas de las penas siguientes:

a) Una multa igual o hasta el doble de la contemplada para la persona física para el hecho ilícito contemplado en la presente ley.

b) La disolución, cuando se trate de un crimen o un delito sancionado en cuanto a las personas físicas se refiere, con una pena privativa de libertad superior a cinco años.

c) La prohibición, a título definitivo o por un período no mayor de cinco años, de ejercer directa o indirectamente una o varias actividades profesionales o sociales.

d) La sujeción a la vigilancia judicial por un período no mayor de cinco años.

e) La clausura definitiva o por un período no mayor de cinco años, de uno o varios de los establecimientos de la empresa, que han servido para cometer los hechos incriminados.

f) La exclusión de participar en los concursos públicos, a título definitivo o por un período no mayor de cinco años.

g) La prohibición, a perpetuidad o por un período no mayor de cinco años, de participar en actividades destinadas a la captación de valores provenientes del ahorro público.

h) La confiscación de la cosa que ha servido o estaba destinada a cometer la infracción, o de la cosa que es su producto.

i) La publicación por carteles de la sentencia pronunciada o la difusión de ésta, sea por la prensa escrita o por otro medio de comunicación.

Párrafo. - Negligencia u Omisión de la Persona Moral. Asimismo, se considerará responsable civilmente a una persona moral, cuando la falta de vigilancia o de control de su representante legal o empleado haya hecho posible la comisión de un acto ilícito previsto en la presente ley.

Artículo 61.- Acciones Administrativas. Nada de lo establecido en la presente ley, impide recurrir a las acciones administrativas que puedan resultar de leyes y reglamentos especiales aplicables.

Artículo 62.- Pago de Indemnizaciones. Sin perjuicio de las sanciones penales y de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales, las personas físicas o morales podrán ser condenadas al pago de indemnizaciones civiles a favor del sujeto pasivo.

g) **Colombia**:

En Colombia, mediante la ley 1.273 del 2009, se modifica el Código Penal, creando un nuevo bien jurídico tutelado y denominado "de la protección de la información y de los datos". Lo que trata de buscar dicha normativa es la preservación integral de los sistemas que tecnológicos de la información y de las redes de comunicaciones. Por medio de esta incorporación, se suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula varios artículos penales que van desde el artículo 269A hasta el artículo 269J. Además, se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".

De acuerdo con la Revista Cara y Sello, durante el 2007, en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de los ciberdelitos. Al respecto es importante también mencionar que esta Ley 1266 de 2008, definió el término dato

personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas a tener un especial cuidado en el manejo de la información de datos personales de sus empleados.

También es importante agregar que el articulo 269H incluye como circunstancia de agravación punitiva, cuando los delitos que se cometieran fueran realizados en circunstancias tales como:

- Por servidor público en ejercicio de sus funciones.
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para si o para un tercero.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

h) **Argentina**:

En Argentina La Ley 26.388 del 2008 no es una ley especial, sino que más bien llega a regular ciertos tipos de delitos informáticos en un cuerpo normativo separado del Código Penal Argentino, con figuras propias y específicas. Es una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del Código Penal

Argentino, con lo que logra regular las nuevas tecnologías como medios de comisión de delitos previstos en el CP.

Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis, ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000). Por lo tanto empresas, personas físicas, instituciones, organismos públicos y demás, a partir de esta Ley deben tomar las medidas necesarias para no ver comprometida su responsabilidad o imagen en la comisión de delitos informáticos, por los que podrán ser castigados con base en un claro fundamento legal.

i) **Brasil**:

En Brasil La Ley 12.737 del año 2012, es una ley reciente, en la que dispone la tipificación de los delitos informáticos y otras como los delitos relacionados con la información personal almacenada en computadoras, el cual prevé penas de seis meses a dos años de prisión por violar correos electrónicos que contengan información y datos de carácter confidencial, ya sean de naturaleza privada o comercial. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, también prevé la pena de tres meses a un año de prisión, además de multa, para quien “invada sistemas informáticos ajenos con el fin de obtener, adulterar o destruir datos o información sin autorización explícita”, además se aplicará la misma pena a quien, ofrezca produzca o venda programas o softwares que permitan la invasión de sistemas y sistemas informáticos ajenos. Tal como sucedió en el año 2011, en el mayor ataque sufrido por órganos gubernamentales

en Brasil que incluyó a sitios de la Presidencia de la República y del Ejército, la pena varía de uno a tres años de prisión.

j) **Chile**:

Siguiendo esta línea, en abril del 2017, Chile firmó el Convenio de Budapest**,** tratado internacional cuyo fin es enfrentar, mediante la creación de leyes acordes con los delitos informáticos a los que demanda la ciberseguridad globalmente.

La Ley 19.223 es una ley de Delitos Informáticos, de acuerdo con su propio título, regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos:

Artículo 1- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2- El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Claramente, los artículos están desactualizados respecto a lo que sucede hoy en internet y específicamente, a la forma en que la gente utiliza internet para realizar cualquier función informática.

La Ley 20.009 del 2005 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. También se encuentra la Ley 18.168 del 2002 (modificada por diferentes normativas) la cual regula de manera general las telecomunicaciones, e incorpora algunos tipos penales sobre la interferencia ilegítima de señales de comunicación.

k) **Guatemala**:

En Guatemala se incorpora dentro del Código Penal el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". En

este capítulo, se mencionan distintas figuras de los delitos informáticos, en especial desde el artículo 274 inciso A hasta el inciso G.

DESTRUCCIÓN DE REGISTROS INFORMÁTICOS

Artículo 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.

ALTERACIÓN DE PROGRAMAS

Artículo 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.

REPRODUCCIÓN DE INSTRUCCIONES O PROGRAMAS DE COMPUTACIÓN

Artículo 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.

REGISTROS PROHIBIDOS

Artículo 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.

MANIPULACIÓN DE INFORMACIÓN

Artículo 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.

USO DE INFORMACIÓN

Artículo 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.

l) **Paraguay**:

Para Paraguay no aparece una legislación especial referida a esta materia en particular. Sin embargo, a partir del 1 de octubre de 2010, entró en funcionamiento la Unidad de Delitos Informáticos y se dieron distintas reformas que sufrió el Código Penal Paraguayo. Se han adaptado algunos delitos con la posibilidad de comisión por medio de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos tales como:

Artículo 174 b.- Acceso indebido a sistemas informáticos.

1°El que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa.

2°Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático.

Artículo 175.- Sabotaje de computadoras.

El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante:

1. Un hecho punible según el artículo 174, inciso 1º.

2. La destrucción, inutilización sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital,

será castigado con pena privativa de libertad de hasta cinco años o con multa. En estos casos, será castigada también la tentativa.

Artículo 188.- Operaciones fraudulentas por computadora

El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. Programación falsa;

2. Utilización de datos falsos o incompletos;

3. Utilización indebida de datos;

4. Otras influencias indebidas sobre el procesamiento, y con ello, perjudicará el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

m) **Puerto Rico**:

En Puerto Rico, igualmente no se ha encontrado legislación especial al respecto. Sin embargo, en este país se ha optado por la modificación de los tipos penales clásicos, adaptándolos en la comisión que ocurre por medio de las nuevas tecnologías. A su vez, mediante la Ley de Espionaje Cibernético N.º 1165 del 2008 sí se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje.

n) Costa Rica:

En cuanto a Costa Rica, se puede decir que mediante la Código de Normas y Procedimientos Tributarios (Ley No. 4755) de 1995, se establece el nacimiento de la regulación del delito informático, mediante los siguientes artículos:

Artículo 94.- Acceso desautorizado a la información

Será sancionado con prisión de uno a tres años quien, por cualquier medio tecnológico, acceda a los sistemas de información o bases de datos de la Administración Tributaria, sin la autorización correspondiente.

Artículo 95.- Manejo indebido de programas de cómputo

Será sancionado con pena de tres a diez años de prisión, quien, sin autorización de la Administración Tributaria, se apodere de cualquier programa de cómputo, utilizado por ella para administrar la información tributaria y sus bases de datos, lo copie, destruya, inutilice, altere, transfiera, o lo conserve en su poder, siempre que la Administración Tributaria los haya declarado de uso restringido, mediante resolución.

Artículo 96.- Facilitación del código y la clave de acceso

Será sancionado con prisión de tres a cinco años, quien facilite su código y clave de

acceso, asignados para ingresar a los sistemas de información tributarios, para que otra persona los use.

Artículo 97.- Préstamo de código y clave de acceso

Será sancionado con prisión de seis meses a un año quien, culposamente, permita que su código o clave de acceso, asignados para ingresar a los sistemas de información tributarios, sean utilizados por otra persona.

En cuanto la **Ley General de Aduanas (Ley No. 7557)** se asemeja mucho a la de Código de Normas y Procedimientos Tributarios, seguramente debido a que se puso en vigencia por los legisladores pocos meses después en el año 1995. En este Código, en la sección III en su capítulo II se incluye el denominado “Delitos Informáticos”, el cual contiene y contempla en sus artículos 221 y 222 las siguientes conductas delictivas:

Articulo 221.- Delitos informáticos

Será reprimido con prisión de uno a tres años quien:

a) Acceda, sin la autorización correspondiente y por cualquier medio, a los sistemas informáticos utilizados por el Servicio Nacional de Aduanas.

b) Se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación y sus bases de datos, utilizados por el Servicio Nacional de Aduanas, siempre que hayan sido declarados de uso restringido por esta autoridad.

c) Dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos diseñados para las operaciones del Servicio Nacional de Aduanas, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona.

d) Facilite el uso del código y la clave de acceso asignados para ingresar en los sistemas informáticos. La pena será de seis meses a un año si el empleo se facilita culposamente.

Articulo 222.- Agravante

La pena será de tres a cinco años cuando, en alguna de las causales del artículo anterior, concurra una de las siguientes circunstancias:

a) Intervengan en el hecho tres o más personas, en calidad de autoras.

b) Intervenga, en calidad de autor, instigador o cómplice, un funcionario público en ejercicio de sus funciones, con ocasión de ellas o con abuso de su cargo.

En la **Ley de la Administración Financiera de la República y Presupuestos Públicos (Ley No. 8131),** la cual entra en vigencia en el 2001 donde contempla en

el título X “Del Régimen de Responsabilidad” un artículo único y exclusivo referente al Delito Informático:

Artículo 111.-Delito informático.

Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera de Proveeduría, alguna de las siguientes acciones:

a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información, programas o bases de datos de uso restringido.

b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.

En este artículo se establecen varias conductas típicas con el fin de proteger la información, las bases de datos y los programas de la Administración Financiera de Proveeduría. Se protege, de forma muy similar a las dos leyes anteriormente mencionadas, también, el bien jurídico que trata de resguardar es el mismo, la

sanción e incluso las acciones delictivas son semejantes o iguales, y de la misma manera el sujeto activo.

En el caso de la **Ley General de Telecomunicaciones (Ley No. 8642)** como parte del paquete del Tratado de Libre Comercio entre Estados Unidos y Centro América (CAFTA), el legislador costarricense establece, de una forma correcta y acertada, una regulación en esta materia, cuando primeramente no lo hace con base en el derecho penal, sino que la sanción la enfoca en lo civil, de esta manera hace que con esta normativa, lo que viene a prohibir son las comunicaciones no solicitadas por medios electrónicos, de sistemas tales como: de llamada automática por voz, correo electrónico, fax, o cualquier otro dispositivo, que tenga fines de una venta directa.

Por lo tanto, en el Título V, se encuentra el régimen sancionatorio en cuanto Infracciones y Sanciones de la siguiente manera, a partir del artículo 65 y concordantes:

Articulo 65.- Potestad sancionatoria

Sin perjuicio de la responsabilidad penal o civil, a la Sutel le corresponde conocer y sancionar las infracciones administrativas en que incurran los operadores o proveedores y también los que exploten redes de telecomunicaciones o presten servicios de telecomunicaciones de manera ilegítima.

Para determinar las infracciones y sanciones a las que se refiere el presente capítulo, se estará a lo dispuesto en el libro segundo de la Ley general de la Administración Pública, N.° 6227, de 2 de mayo de 1978, y sus reformas.

Articulo 66.- Medidas cautelares

Durante el procedimiento, la Sutel podrá imponer las medidas cautelares necesarias para asegurar el resultado de un procedimiento sancionatorio o evitar que se pueda comprometer la actividad prestada, así como la integridad de instalaciones, redes, equipos y aparatos.

Cuando tenga indicios claros acerca de la operación ilegítima de redes o la prestación ilegítima de servicios de telecomunicaciones, la Sutel podrá imponer como medida cautelar el cierre de establecimientos, la clausura de instalaciones o la remoción de cualquier equipo o instrumento. Para ejecutar estas medidas se dispondrá del auxilio de la Fuerza Pública.

La Sutel, mediante resolución fundada y previa audiencia a los interesados, debe resolver si confirma, modifica o revoca la medida adoptada en un plazo máximo de dos meses, contado a partir del inicio del procedimiento.

Articulo 67.- Clases de infracciones

Las infracciones en materia de telecomunicaciones pueden ser muy graves o graves.

a) Son infracciones muy graves:

1) Operar y explotar redes o proveer servicios de telecomunicaciones sin contar con la concesión o autorización correspondiente.

2) Usar o explotar bandas de frecuencias del espectro radioeléctrico sin la correspondiente concesión o permiso.

3) Usar o explotar bandas de frecuencias del espectro radioeléctrico en violación a lo dispuesto en el Plan nacional de atribución de frecuencias.

4) Incumplir la obligación de contribuir con Fonatel.

5) Incumplir las obligaciones de acceso y servicio universal impuestas de conformidad con esta Ley.

6) Ceder o aceptar la cesión de concesiones sin la aprobación correspondiente.

7) Incumplir las instrucciones adoptadas por la Sutel en el ejercicio de sus competencias.

8) Negarse a entregar la información que de conformidad con la ley requiera la Sutel, así como ocultarla o falsearla.

9) Incumplir la obligación de facilitar el acceso oportuno a las instalaciones esenciales y poner a disposición de los operadores y proveedores información técnica relevante en relación con estas instalaciones.

10) Incumplir la obligación de acceso o interconexión y las demás obligaciones que de ella se deriven.

11) Suspender el acceso o la interconexión sin autorización de la Sutel.

12) Cobrar a los usuarios finales tarifas distintas de las fijadas por la Sutel, cuando corresponda.

13) Realizar las prácticas monopolísticas establecidas en esta Ley.

14) Realizar una concentración sin la autorización a que se refiere esta Ley.

15) Utilizar la información de los usuarios finales para fines no autorizados en la ley.

16) Violar la privacidad o intimidad de las comunicaciones de los usuarios finales.

17) Incumplir las medidas cautelares adoptadas por la Sutel.

18) Incumplir, de manera reiterada, las infracciones graves establecidas en el inciso b) de este artículo.

b) Son infracciones graves:

1) Operar las redes o proveer servicios de telecomunicaciones en forma distinta de lo establecido en la concesión o autorización correspondiente.

2) Incumplir las normas técnicas que resulten aplicables de conformidad con la ley.

3) Incumplir las obligaciones derivadas de los derechos de los usuarios a que se refiere esta Ley.

4) Omitir la resolución de las reclamaciones de los usuarios finales, en el plazo establecido en esta Ley.

5) Incurrir en prácticas de competencia desleal, de conformidad con el artículo 17 de la Ley N.° 7472, Promoción de la competencia y defensa efectiva del consumidor, de 20 de diciembre de 1994.

6) Producir daños a las redes y los sistemas de telecomunicación por el mal uso y funcionamiento de aparatos terminales, equipos y sistemas de su propiedad.

7) Utilizar sistemas de llamada automática por voz, fax o correo electrónico u otros dispositivos en contravención de (sic) lo dispuesto en esta Ley.

8) Emitir señales falsas y engañosas, así como producir interferencias o perturbaciones graves a las redes o servicios de telecomunicaciones.

9) Utilizar equipos en forma distinta de la autorizada, así como darles un mantenimiento inadecuado de manera que se ponga en peligro personas o propiedades y siempre que no se constituya una infracción de mayor gravedad.

10) No mantener actualizada ni custodiada la información requerida por la Sutel.

11) Cualquier acción en contra de lo dispuesto en esta Ley, los reglamentos u otras obligaciones contractuales, que por su naturaleza, daño causado y trascendencia no se considere como infracción muy grave.

Artículo 68. Sanciones por infracciones

Las infracciones serán sancionadas de la siguiente manera:

a) Las infracciones muy graves serán sancionadas mediante una multa de entre cero coma cinco por ciento (0,5%) y hasta un uno por ciento (1%) de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior.

b) Las infracciones graves serán sancionadas mediante una multa de entre cero coma cero veinticinco por ciento (0,025%) y hasta un cero coma cinco por ciento (0,5%) de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior.

Cuando un operador o proveedor no haya obtenido ingresos brutos o se encuentre imposibilitado para reportarlos, la Sutel utilizará como parámetro para la imposición de sanciones el valor de sus activos.

En el caso de las infracciones referidas en el inciso a) del artículo anterior que, a juicio de la Sutel, revistan gravedad particular, esta Superintendencia puede imponer como sanción una multa de un uno por ciento (1%) y hasta un diez por ciento (10%) de las ventas anuales obtenidas por el infractor durante el ejercicio fiscal anterior, o entre un uno por ciento (1%) y hasta por un diez por ciento (10%) del valor de los activos del infractor.

En el caso de que no se pueda aplicar la sanción sobre las ventas o los activos, la Sutel utilizará como parámetro para la imposición de sanciones los ingresos presuntos del período, tomando en cuenta los ingresos brutos promedio de períodos anteriores y los ingresos promedio del período anterior de otros operadores o proveedores que desarrollen actividades económicas y comerciales similares.

Para efectos de imponer la sanción, la Sutel deberá valorar si el infractor forma parte de un grupo económico, de conformidad con lo definido en el artículo seis de esta Ley. En este caso, la sanción será impuesta con base en el ingreso bruto o las ventas anuales, según sea el caso, de las empresas que conforman el grupo.

Articulo 69.- Cierre de establecimientos y remoción de equipos

Con el objetivo de garantizar la integridad y calidad de la red y los servicios de telecomunicaciones, así como la seguridad de los usuarios, la Sutel podrá imponer como sanción, en el caso de las infracciones muy graves, el cierre definitivo de un establecimiento y la clausura de sus instalaciones, la remoción de cualquier equipo o instrumento que permita la operación de redes o la prestación de servicios de telecomunicaciones en forma ilegítima, o ponga en riesgo la integridad de las instalaciones, redes, equipos y aparatos. Para ejecutar estas medidas se dispondrá del auxilio de la Fuerza Pública.

Articulo 70.- Criterios para la aplicación de las sanciones

La Sutel aplicará las sanciones por resolución fundada. Estas se aplicarán en forma gradual y proporcionada tomando en consideración los siguientes criterios: la mayor o menor gravedad de la infracción, el tiempo en que se cometió la infracción, la reincidencia, el beneficio obtenido o esperado con la infracción, el daño causado y la capacidad de pago del infractor.

Para imponer las sanciones, la Sutel debe respetar los principios del debido proceso, la verdad real, el impulso de oficio, la imparcialidad y la publicidad.

Para establecer la verdad real, la Sutel podrá prescindir de las formas jurídicas adoptadas por los operadores o proveedores que no correspondan con la realidad de los hechos investigados.

Y por último, se analiza muy brevemente la **Ley 9048 "Reforma de varios artículos y modificación de la sección VIII denominada delitos informáticos y conexos, del título VII del Código Penal"** del 10 de julio del 2012 en la que se crean varios tipos penales como la suplantación de identidad, espionaje electrónico, falsificación y clonación de sitios web, la propagación de *malware* y envíos de *spam*. A pesar de que viene a aportar grandes avances en la lucha contra el cibercrimen, deja a su vez con un sin sabor a la población y a ciertos sectores gremiales, que toman parte de esta ley, como una mordaza a los temas de Investigación periodística en temas políticos y de corrupción, esto dio lugar a que una acción de inconstitucionalidad tomara lugar contra la Ley 9048, y que resultara en la sentencia 2015-5615, del 22 de abril, en la que la Sala Constitucional, por mayoría, acordó resolver parcialmente con lugar. La decisión de los magistrados consistió en anular la frase: *cuando los datos sean de carácter público* contenida en el inciso b), del artículo 196 bis, para los magistrados, ese inciso antes citado es violatorio al derecho a la información y al principio de transparencia, "ya que lo único limitado a la persona, es el acceso a aquellos documentos o correspondencias señaladas como secreto de Estado o que contengan datos personales de acceso restringido".

3.4.3 Legislación Comparada en Países de Europa

España:

En España, mediante la Ley Orgánica 1/2015 que modifica a la Ley Orgánica 10/1995, del Código Penal, se adoptan mejoras técnicas para ofrecer un sistema penal más ágil y eficiente, se introducen nuevas figuras delictivas, se adecuan tipos penales ya existentes, con la finalidad de ofrecer una garantía de respuesta más efectiva a las nuevas formas del cibercrimen. Gran parte de esta reforma está enfocada en dar cumplimiento a los compromisos internacionales adquiridos por España, en los que se encuentra una mejora técnica en la regulación de la responsabilidad penal de las personas jurídicas, del cual asume ciertas recomendaciones que habían sido realizadas por algunas organizaciones internacionales en esta materia. Es importante señalar que España ha sido un referente en el estudio de esta tesis, por sus alcances legislativos que ha promulgado con esta reforma en los delitos informáticos. Es pionera en la responsabilidad de las personas jurídicas y en el alcance de las obligaciones que conlleva ese deber de control que condiciona, de modo general, las dimensiones de la persona jurídica como lo señalan los siguientes artículos precisamente en este tema:

Artículo 264 quater

1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos,

programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias:

1.ª Se hubiese cometido en el marco de una organización criminal.

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.

3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A (sic) estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. (utilización programas informáticos o usando contraseñas)

Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Por su parte el **artículo 31 bis** del Código Penal requiere solamente que se dé una omisión de los deberes de control y vigilancia correspondientes a la persona jurídica para responsabilizar cuando la actividad ciber delictiva se cometa por parte de un subordinado.

A su vez, parte de las penas interdictivas que el artículo 33.7 del CP hace mención para la persona jurídica para su aplicación son las siguientes: a) disolución de la persona jurídica; b) suspensión de sus actividades por un plazo que no podrá exceder de cinco años; c) clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años; d) prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito; e) inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años; f) intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

También se establece debidamente como exención de responsabilidad penal a las personas jurídica si se pasara por la figura del compliance penal, donde se compruebe toda la realización de los protocolos contemplados en el **art. 31 bis** del Código Penal español.

Alemania:

En Alemania tras un largo debate que inicio en la década de los 70s, hizo que consecuentemente se creara la "Segunda Ley de Lucha contra la Criminalidad Económica" de 1986, en la que se introdujeron nuevas figuras penales que se mencionan a continuación.

Espionaje de datos (sección 202 a)

Estafa informática (sección 263 a)

Falsificación de datos probatorios (sección 269) junto a modificaciones complementarias del resto de falsedades documentales, como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (secciones 270, 271, 273)

Alteración de datos (sección 303 a) es ilícito inutilizar, cancelar, o alterar datos, inclusive la tentativa es punible.

Sabotaje informático (sección 303 b) Destrucción en la elaboración de datos de especial significado por medio de deterioro, Inutilización, destrucción, eliminación o modificación de un sistema de datos. Así mismo es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito (sección 266b).

Francia:

Pasando a Francia, en enero de 1988, se dicta la **Ley número 88-19** relativa al fraude informático.

Acceso fraudulento a un sistema de elaboración de datos (462-2). - En este artículo se sanciona tanto el acceso restringido al sistema, como la permanencia en él, y aumenta la sanción correspondiente si de ese acceso resulta la modificación o extracción de los datos contenidos en el sistema, o si del mismo resultara la alteración del funcionamiento del sistema.

Sabotaje informático (462-3). - Se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos (462-4). - Se sanciona a quien con intención y con menosprecio de los derechos de los demás, introduzca datos en un sistema automatizado de datos o suprima, modifique los datos que este contiene o los modos de transmisión.

Falsificación de documentos informatizados (462-5). - Se sanciona a quien de cualquier modo, falsifique documentos informatizados con intención de causar un perjuicio a otro.

Uso de documentos informatizados falsos (462-6) Se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Unión Europea:

En la Unión Europea, recientemente la Directiva 2016/1148, está destinada a garantizar un nivel de seguridad común en la Unión, entre los sistemas de información tecnológicos. Parte de los puntos que designa es la cooperación y comunicación transfronteriza, menciona y aconseja que cada Estado miembro designe un punto de contacto único nacional el cual se encargará de las coordinaciones necesarias para enfrentar una situación, y a su vez señala que se debe disponer de los recursos técnicos, financieros para alcanzar los objetivos que tiene la Directiva.

La Directiva, a fin de promover un alto nivel de seguridad informática y redes, menciona que se intercambiarán prácticas y conocimientos teóricos donde haya un asesoramiento efectivo en las instituciones públicas y privadas, así como órganos y organismos de la Unión Europea. Entre los Estados miembros se ejecutan ejercicios de simulación en tiempo real relacionados con incidentes tecnológicos para comprobar el grado de preparación y respuesta con que cuenta cada Estado en su seguridad informática y de redes de comunicación.

También existen medidas de gestión del riesgo, cuya es determinar los riesgos de incidentes, gestionarlos, prevenir, detectar y mitigar sus repercusiones. Parte de las

acciones es que se debe notificar sin demoras a la autoridad competente o al CSIRT (siglas de término en inglés Computer Security Incident Response Teams), cualquier incidente importante en el que se hallen efectos significativos en la continuidad de los servicios esenciales que se presten, para tomar las medidas correspondientes de carácter institucional, o nacional según corresponda.

En relación con la ciberseguridad, en el campo técnico y organizativo existen otras leyes, establecidas por el **Reglamento Europeo de Protección de Datos 2016/679**, para los que también hay que tomar en cuenta otro tipo de reglas internacionales, en especial las relacionadas con el traspaso internacional de datos, como el **Privacy Shield**.

3.5 MECANISMOS Y PARÁMETROS PREVENTIVOS PARA LA APLICACIÓN DENTRO DEL SENO ORGANIZACIONAL DE LA EMPRESA

En los últimos tiempos, gracias al creciente número de actos ciber delictivos que se dan dentro de las empresas de forma global, se ha visto reflejado a su vez en nuevos productos que ofrecer en el mercado, en el que muchas han procurado preferiblemente la implantación de sistemas de vigilancia y prevención de estos delitos, mediante programas llamados *corporate compliance* como ya se hace en algunos países donde está política de seguridad informática ha sido efectivamente introducida mediante normas incluidas en sus legislaciones.

Para entender un poco mejor qué es el *corporate compliance*, se debe saber primeramente que es un conjunto o grupo de procedimientos y lineamientos de buenas prácticas, que las organizaciones corporativas adaptan a lo interno para

trabajar en la identificación y clasificación de los riesgos o peligros operativos, con la posibilidad de poder exonerarse legalmente en casos donde no se haya podido evitar el acto delictivo, también, a su vez, se establecen mecanismos internos de gestión, prevención, control y respuesta frente a situaciones o actos que pongan en riesgo la información, datos, patrimonio y otras áreas que podrían repercutir en afectaciones a terceros. Con ello se previenen riesgos que pueden llevar a consecuencias como un daño reputacional, grandes multas y sanciones que pongan en peligro la continuidad operacional por un periodo de tiempo, exclusión de licitaciones, responsabilidades penales y civiles, disolución de la persona jurídica, clausura de sus locales y establecimientos por un plazo entre otras.

3.5.1 Proceso de Elaboración del *Corporate Compliance* en la Persona Jurídica

En los procesos de implementación en las empresas de este tipo de sistemas evaluativos de prevención, se deben tomar en cuenta ciertos lineamientos que vayan acorde con los sistemas tecnológicos que en ella se utilicen, así como la valoración de las posibles pérdidas económicas y afectaciones que puedan ocurrir en ciertas áreas donde se estipulen, sean las más críticas o más vulnerables, en las que se pueda cometer algún tipo de delito organizacional en cualquier nivel jerárquico de los sistemas de seguridad informáticos, y que se encuentren bajo la supervisión o manejo de personas con alto nivel de acceso a los sistemas de automatización de datos de la empresa.

En un primer paso, se deben analizar los riesgos jurídicos, para ello es necesario contratar una auditoria legal, la que primeramente deberá hacer unas entrevistas con los responsables de cada área, se discutirán los riegos y medidas de control que ya se encuentran establecidos en la empresa auditada.

Tras esta primera revisión, y con base en un análisis de los datos recaudados, se puede ver que tan sensible es la información que se maneja en los sistemas que se trata de proteger, confidencial, intermedia o de máximo nivel de criticidad, cuáles son sus vulnerabilidades considerando áreas deficientes de seguridad y que puedan resultar transgredidas, después se sigue con la propuesta de una mejora de las medidas existentes y a su vez implementación de las nuevas, una vez detectadas las amenazas, riesgos y las personas que tendrán solamente acceso a ella.

La seguridad informática de las empresas depende en gran parte de los usuarios (empleados) que deben conocer las políticas de seguridad, a su vez, tener una perspectiva general de las reglas y procedimientos de implementación que deben saber para enfrentar los riesgos identificados en las diferentes áreas de los sistemas de información.

Se deben definir acciones y las personas que se deben contactar en los casos que se detecte una amenaza por medio de un canal de comunicación especifico. Por eso, deben existir mecanismos de seguridad, tanto físicas como lógicas, que se adapten de acuerdo con las necesidades de la empresa y el uso de los empleados que las controlan, para los que igualmente se debe implementar un procedimiento para las actualizaciones que deben existir en los programas y de las copias de

seguridad constantes de los equipos tecnológicos, para en un dado caso que exista un suceso por el que se pierda parte de la información, esta pueda ser recuperada luego del incidente, por lo que es necesario siempre tener toda esta documentación actualizada y a mano de los usuarios.

A continuación, se desarrollan algunos mecanismos básicos que las organizaciones e instituciones públicas y privadas deberían tener e implementar en su entorno operativo en Costa Rica.

Tecnologías de monitoreo a distancia: vigilancia y las cámaras de seguridad, que sirven para observar quiénes ingresan a determinada área, con las que se registra hora y día, además, se pueden agregar *badge* a los colaboradores de la empresa para registrar sus movimientos por medio de ella.

Encriptación o cifrado: este mecanismo consiste en un procedimiento del cual se somete un documento, mensaje o información a un algoritmo de cifrado que transforma su contenido en ilegible. Solo podrán leerla las personas con la clave correcta, es un mecanismo que aumenta los niveles de seguridad.

Entrenamiento y conocimiento de los colaboradores sobre las medidas de seguridad de la empresa y su implementación efectiva: Los estándares de seguridad permiten la aplicación de prácticas y entrenamientos en las políticas y reglamentos que deben ser utilizadas e integradas correctamente en la empresa, además se utilizará un conjunto de acciones, metodologías, técnicas y herramientas, las cuales serán aplicadas y probadas. La seguridad debe ser una responsabilidad gerencial y esta tiene que aparecer en los objetivos de la

organización. Una vez implementada, se debe dar respuesta a los incidentes o actos que vayan en contra de estas políticas de forma inmediata con procedimientos que deben estar en las herramientas automatizadas de la misma empresa.

Auditorías: el realizar un continuo chequeo de los sistemas para detección de anomalías o cualquier información no autorizada, es primordial asegurarse que los mecanismos de seguridad que se están implementando en la empresa, funcionan de manera correcta, debido a que muchas veces, por exceso de confianza, las personas a cargo de la vigilancia y control de esta seguridad pueden ser responsables de manera culposa en el daño que se realice y que pudo haber sido previsto.

Implementación de sistemas de seguridad en las redes informáticas de la empresa: Los conocidos *Firewalls* o “cortafuegos” son herramientas tecnológicas configuradas e instaladas en la red para evitar o bloquear el acceso a personas no autorizadas a cierta información crítica o programas esenciales para la compañía; con ellas, se va a filtrar el tráfico en la red de manera interna y externa.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

La prevención y detección de los delitos informáticos en las personas jurídicas constituye una labor ardua y continua que requiere de forma constante actualizaciones en sus procesos, como así mismo en sus legislaciones para poderle hacer frente a esta poderosa herramienta que es la tecnología. Muchos países ya tienen en sus sistemas penales y civiles una manera de responsabilizar a los entes colectivas de las empresas que se benefician de estos actos ciber delictivos, cuyo desarrollo social de los últimos años ha obligado al derecho a innovarse de forma constante, principalmente por la introducción de las nuevas tecnologías de la información y comunicación en las empresas e instituciones costarricenses.

Conforme las actividades digitales toman cada vez más protagonismo en la vida cotidiana, las personas físicas y jurídicas se ven expuestas a nuevos riegos, por lo que mantener un ambiente de seguridad para los usuarios, debe ser el principal reto en esta materia para el tráfico jurídico en Costa Rica.

A continuación se presenta, como resultado de una amplia investigación, una serie de apreciaciones y hechos relevantes resultado del trabajo realizado, el cual se ha desarrollado a lo largo del presente estudio.

- En la formulación del problema de esta tesis se planteó si era adecuado adaptar penas interdictivas, no solo a los colaboradores de la empresa, sino también a los administradores o representantes de las personas jurídicas que realicen ciberdelitos, y se concluyó que sí es importante establecer una norma que castigue de manera adecuada, lo mismo que de forma preventiva, actos que puedan ir en contra de las políticas de seguridad informática empresarial.

- Parte de los objetivos generales y objetivos que se plantearon en este documento dieron como resultado la importancia de incluir medidas preventivas tales como: multas, disolución de la persona jurídica, suspensión de actividades, clausura de locales por plazos, prohibición de realizar actividades en el país, intervención judicial, prohibición de

participar en concursos para concesiones etc. De esta manera, habrá mayor cuido y vigilancia, así como diligencia a la hora de tratar sistemas de información automatizados que almacenen información crítica y el patrimonio de muchos de sus usuarios.

- Uno de los puntos claves del desarrollo de este estudio, fue indagar la viabilidad jurídica en la legislación costarricense de una adecuada integración de normas mediante la base de la legislación comparada, con la que se aplique adecuadamente la responsabilidad a las personas jurídicas que comentan delitos informáticos, y se determinó que mediante mejoras técnicas de conocimiento de los legisladores y funcionarios judiciales es posible impulsar normas que ofrezcan verdaderamente una garantía de respuesta efectiva contra las nuevas formas del ciber crimen y que se enfoque en cumplir a cabalidad los compromisos internacionales adquiridos en esta materia. Es por esto por lo que surge como primordial, la valoración de una posible reforma normativa que estipule sistemas preventivos y de detección que eviten posibles lesiones a los bienes jurídicos protegidos en los delitos

informáticos, y una debida comunicación entre el sector privado y público, para que haya una cooperación mutua que permita un desarrollo amigable entre ambos sectores en cuanto la seguridad informática, con lo la persona jurídica dejará de esconderse en ese velo de impunidad que aún lo protege y que prolifera cada día más, al no estar regulado debidamente.

- La falta de información y de actualización sobre esta materia en los juristas y en la población en general en Costa Rica, pone de manifiesto que es importante implantar leyes especiales sobre delitos informáticos tomando como marco de referencia al derecho comparado para su implementación, a su vez, crear capacitaciones en las universidades que incluyan en sus carreras informáticas y jurídicas materias de derecho informático para la creación de futuros profesionales, que conozcan la seguridad que debe mantenerse acorde con los avances tecnológicos en las respectivas instituciones y empresas del país una vez que se asuman políticas y normas que verdaderamente enfrenten estos actos delictivos.

- Se determina que los delitos informáticos en la persona jurídica trabajan de diferente manera, ya que usualmente son ocupacionales, ocurren en el seno de la organización empresarial donde el sujeto activo en la mayoría de las veces cuenta con una posición de poder. Son de oportunidad, se conoce cómo, cuándo y dónde realizarlo en el momento preciso, tienden a afectar la imagen de la empresa con consecuentes perdidas económicas.
- Proliferan cada día más en países como Costa Rica, donde no existe una clara regulación en esta materia que responsabilice al ente colectivo. Algunos buscan afectar a la competencia accediendo de forma ilícita a los sistemas, buscando información que pueda ser copiada o utilizada para fines propios de ganar un mejor posicionamiento en el mercado.

4.1.1 Conclusiones Generales

- La cibersociedad de la cual este país ya forma parte y donde aquellos acontecimientos culturales y jurídicos en torno a esta materia se han modificado, de los que Costa Rica apenas está comprendiendo las

implicaciones y efectos sociales, políticos y económicos que pueden darse en los delitos informáticos.

- El Sistema Judicial Costarricense debe conformarse en su departamento de Delitos Informáticos, no solamente por informáticos sino también por abogados con conocimientos en esta área y tecnología, suficientemente capaces para poder enfrentar estos actos y que además, el Estado ofrezca recursos económicos ciertos, y una verdadera persecución de los hechos para obtener resultados que permitan establecer penas que vayan acorde con la gravedad de la lesión.

- Los indicios y porcentajes de ataques cibernéticos en el país, presentados en este estudio, ocurridos dentro del seno de la organización empresarial, demuestran la poca importancia que se le brinda a este tipo de delitos, y el poco desarrollo de normas y leyes especiales, lo que hace que las personas jurídicas se mantengan detrás de un velo de impunidad.

- Se realizó un análisis a nivel internacional de otras legislaciones del continente americano y europeo, y se encontró un tratamiento jurídico más avanzado en ciertos sectores, lo que deja claro que se debe seguir avanzando y luchando por mejoras en la legislación penal y civil, en las que se efectué una correcta adaptación de sistemas de seguridad para que se deje de exponer a todos los ciudadanos y empresas a un ambiente de desprotección que se mantiene muy amplio aún en Costa Rica.

- Los bienes jurídicos más importantes en los delitos informáticos, primeramente se encuentran en la información, la cual es almacenada, tratada y trasmitida mediante sistemas automatizados de datos. La lesión a un bien jurídico como este, podría ocasionar un riesgo potencial a un número indefinido e indeterminado de víctimas en los ciber delitos, a su vez, aparece otro bien jurídico muy crítico y de gran valor económico que se debe proteger, que es el *software* o programa computacional que se puede encontrar bajo el poder de disposición de una persona y empresa del cual requiere de sus servicios. Estos bienes

jurídicos son equiparados a obras literarias, científicas, artísticas, y una afectación a estos puede verse como un daño a la propiedad intelectual.

- Es sabido que la persona jurídica no es sino un patrimonio organizado en torno a una actividad, el cual está dirigida, organizada y administrada por personas físicas, por lo que es imposible hacer a un lado la titularidad de las conductas que recaen sobre la persona jurídica, en que el autor material es exclusivamente la persona física. La persona jurídica no debería ser considerada más que un instrumento que se utiliza para la realización de actos delictivos en el ámbito informático.

- El *Corporate Compliance* debe ser introducido por parte del Estado Costarricense en el ámbito jurídico por razones estratégicas, debido a la falta de recursos que se posee para controlar los ciberdelitos y la compleja estructura empresarial que incentiva cada vez más la proliferación de actos delictivos. La posible exoneración de responsabilidad civil y penal se podría alcanzar por medio de la instauración de estas reglamentaciones, que se estipule una ley especial en el núcleo de la persona jurídica, que colabore con la supervisión del

funcionamiento y cumplimiento de ciertos parámetros en el modelo de prevención implantado que se vaya a requerir.

4.2 RECOMENDACIONES

Para finalizar el trabajo de tesis, este capítulo se dedicará a mostrar las recomendaciones con base en el estudio realizado sobre el derecho comparado en materia informática y de las personas jurídicas, entre otros temas que se citan a continuación.

1 Valorar una de posible reforma en la legislación actual que regula los delitos informáticos, que no solo sea en la materia penal, que se incluya la civil, para que se pueda construir una ley especial que contenga una protección integral de los sistemas tecnológicos en las instituciones y empresas públicas y privadas.

2 Que se brinde un plan estratégico a nivel nacional que impulse políticas y estudios en los métodos de seguridad informática, para fomentar una

cultura de prevención y responsabilidad en los entes colectivos de las empresas.

3 Para hacerle frente a esta herramienta tan poderosa como lo es la tecnología, Costa Rica debe estar a la vanguardia con las herramientas jurídicas adecuadas. Como parte de esta recomendación, se debe buscar la manera incluir el Artículo 12 del Convenio de Budapest, que responsabiliza a las personas jurídicas de una forma armoniosa, para que sea posible su adaptación al marco legal costarricense.

4 Concientizar a las personas físicas que integran a las personas jurídicas, así como sus representantes y administradores del seno empresarial para que incluyan medidas preventivas y políticas de seguridad que pongan en práctica una adecuada vigilancia de los sistemas tecnológicos de información, y así evitar posibles lesiones a bienes jurídicos y usuarios que utilizan estos servicios.

5 Fortalecer más la cooperación internacional en esta materia, en la que las personas jurídicas en muchas áreas de la región, siguen impunes antes los actos que estos siguen realizando, debido al velo de protección en se encuentran al no estar regulados debidamente en el Derecho Informático.

6 Para poder lograr una efectiva inclusión de la responsabilidad de las personas jurídicas en el ordenamiento jurídico costarricense, se debe plantear de una forma íntegra, que se tomen en cuenta todos los factores que intervienen en las variadas formas societarias reguladas en el marco legal costarricense.

7 Es importante analizar el derecho comparado en la función legislativa, para poder asignar una responsabilidad a las personas jurídicas en los delitos informáticos, y que al encontrar semejanzas y diferencias en distintos ordenamientos jurídicos, sea más sencillo poder elaborar y mejorar el del país. A su vez, los legisladores deben saber que sin el auxilio de esta materia no es posible elaborar leyes que vayan acorde

con los avances tecnológicos en el mundo, que otorgue como se mencionó antes, una seguridad jurídica en el entorno empresarial.

BIBLIOGRAFÍA

Corbetta, P. (2007). *Metodología y Técnicas de Investigación Social, 2° ed.* México: McGraw Hill.

Adalid Medrano, Entrevista, 15 de noviembre del 2018.

Sautu, R. (2009). *El Marco Teórico en la Investigación Cualitativa, Controversias y Concurrencias Latinoamericanas.*

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

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

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

LEY 1273. *De la Protección de la información y de los datos.* Publicado en el Diario Oficial. Colombia, 5 de enero,2009.

Fiscal Impuestos (2017) *9 cosas que necesitas saber sobre la responsabilidad penal de las personas jurídicas.* Recuperado de: https://www.fiscal-impuestos.com/9-cosas-necesitas-saber-responsabilidad-penal-personas-juridicas.html

KNORR, Jolene Marie, SAUMAN, Marcelo Roldan. *La Protección del Consumidor en el Comercio Electrónico.* Investigaciones Jurídicas S.A., San José, Costa Rica, 2001

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.

Informática Juridica.com (2014) *Posibles sujetos de los delitos informáticos.* Recuperado de: http://www.informatica-juridica.com/trabajos/posibles-sujetos-de-los-delitos-informaticos/

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, 6 de julio 2016

El Financiero (2017) *La responsabilidad de los directores.* Recuperado de: https://www.elfinancierocr.com/economia-y-politica/la-responsabilidad-de-los-directores/XSKPYDBNUJAT7LJYWQSK3LHTRM/story/

Enrique Bacigalupo Zapater (2002) *Documentos Electrónicos y Delitos De Falsedad Documental.* Recuperado de: http://criminet.ugr.es/recpc/recpc_04-12.pdf

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.

Ecija Abogados (2010) *Compliance. Cumplimiento Normativo y Seguridad en la Empresa.* Editorial Aranzadi

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

Mayer, L. (2017). *El Bien Jurídico Protegido en los Delitos Informáticos.* Revista Chilena de Derecho. Volumen 44 (1): 235-260

Ministerio de Justicia. (2015). *Análisis De Derecho Comparado sobre Ciberdelincuencia, Ciberterrorismo y Ciberamenzas al Menor.* Ed. Madrid, España.

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

Ley No. 53-07. *Crímenes y Delitos de Alta Tecnología.* Santo Domingo de Guzmán, República Dominicana, Gaceta Oficial, 23 de abril 2007.

Ley Nº 12.737. *Tipificación Criminal de los Delitos Informáticos.* Brasil, Diario Oficial, 3 de diciembre 2012.

La Ley 26.388. Modificación, Código Penal. Argentina, junio 24 2008

Ley número 88-19, *Fraude Informático*. Francia, 5 de enero 1988

Ley Orgánica 1/2015, Modificación, Código Penal. España

Ley General de Aduanas 7557. Sección III, Capitulo II, Delitos Informáticos.

Costa Rica, 20 de octubre 1995.

GLOSARIO

Derecho comparado: Es una técnica para estudiar el Derecho, caracterizada por contrastar instituciones o figuras jurídicas de distintos ordenamientos con el fin de profundizar en el conocimiento del ordenamiento propio.

CEC: Convención sobre la Ciberdelincuencia o Convenio de Budapest.

Corporate Compliance: es un conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos.

Privacy Shiel: es un certificado nacido en julio de 2016 que necesitan las empresas internacionales cuando quieren tratar con los datos de ciudadanos europeos.

CSIRT: siglas de término en inglés Computer Security Incident Response Teams.

CP: Código Penal

SUTEL: Superintendencia de Telecomunicaciones de Costa Rica

CAFTA: Tratado de Libre Comercio entre Estados Unidos y Centro América

CSI: Instituto de Seguridad en Computadoras

ONU: Organización de las Naciones Unidas

OCDE: Organización de Cooperación y Desarrollo Económico

IT: Tecnología Informática

Commonwealth: Mancomunidad de Naciones, antiguamente Mancomunidad Británica de Naciones, es una organización compuesta por 53 países soberanos independientes y semiindependientes que, con la excepción de Mozambique y Ruanda, comparten lazos históricos con el Reino Unido.

ANEXOS

El propósito de este listado de pasos sobre el Corporate Compliance es exponer un breve ejemplo de la metodología que hoy en día se usa en las empresas e instituciones a nivel global que cuentan con sistemas de automatización que contengan información crítica y valiosa para las operaciones informáticas, la asignación de este control puede darse según el puesto de trabajo o función que se realice, el cual puede estar prevista en una ley especial o reglamento.

1. Código ético.
2. Política de prevención y control.
3. Mapa de riesgos.
4. Mapa de controles
5. Protocolo de toma de decisiones.
6. Modelo de gestión de los recursos informáticos.
7. Sistema disciplinario.
8. Canal ético.

9. Estructura de control.

10. Repositorio de evidencias.

11. Actas del Consejo de Administración.

12. Política de bonus.

13. Bonus otorgados por buenas prácticas en materia de compliance.

14. Consultas formuladas al canal ético o al Compliance Officer.

15. Denuncias de incumplimiento a través del canal ético.

16. Sanciones impuestas por incumplimiento del modelo.

17. Evidencias de la existencia, la idoneidad y la eficacia cada control.

18. Cursos presenciales realizados.

19. Cursos de e-learning realizados.

20. Campus de compliance interno o externo.

21. Campañas de sensibilización realizadas.

22. Cursos de refuerzo realizados en el caso de los delitos informáticos que pueden ser cometidos de forma imprudente.

23. Evaluaciones realizadas para comprobar la cultura de los directivos y los subordinados en materia de compliance y principios éticos.

24. Resultados comparativos de las evaluaciones a lo largo del tiempo.

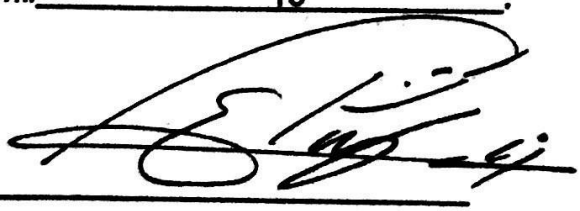
Fuente: Ribas & Asociados, Barcelona, España.

DECLARACIÓN JURADA

Yo Edwin Perez Brenes, mayor de edad, portador de la cédula de identidad número 1-11620312 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 en Derecho, juro solemnemente que mi trabajo de investigación titulado: CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAIS ANTES LA FALTA DE REGULACION ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURIDICAS

_____, 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 17 días del mes de Julio del año dos mil 19.



Firma del estudiante

Cédula: 1-1162-0312

15 de julio de 2019

Señores
Consejo Académico
Universidad Hispanoamericana
Presente

Estimados señores:

La suscrita, **LICENCIADO GERMAN SALAZAR SANTAMARIA**, en mi condición de Director de la tesis para optar por el Grado Académico Licenciatura en Derecho, del estudiante EDWIN PEREZ BRENES denominada **"CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAÍS ANTE LA FALTA DE REGULACIÓN ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURIDICAS"** hago constar por medio de la presente, que he revisado dicha investigación y la misma cumple con los requisitos de forma y fondo que exige el rendimiento de la Universidad, por tanto doy mi aprobación al mismo.

En mi calidad de tutor, he verificado que se han realizado las correcciones durante el proceso de tutorías, y he evaluado los aspectos necesarios relativos a la elaboración del problema, objetivos, antecedentes, marco teórico, análisis de datos, conclusiones y recomendaciones.

a.-	Originalidad del Tema	10%	10%
b.-	Cumplimiento de entrega de avances	20%	20%
c.-	Coherencia entre objetivos, resultados de la investigación.-	30%	30%
d.-	Relevancia de las conclusiones y recomendaciones	20%	20%
e.-	Calidad de detalle del marco teórico	20%	20%
f.-	Total		100%

En virtud de la calificación obtenida, se avala para su lectura el presente trabajo de investigación.

Agradeciendo su atención;

Lic. German Salazar Santamaria
Director de Tesis

CARTA DE LECTOR

San José,

Universidad Hispanoamericana
Sede Llorente
Carrera

Estimado señor

El estudiante Edwin Pérez Brenes, cédula de identidad 1-1162-0312, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAIS ANTE LA FALTA DE REGULACION ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURIDICAS", el cual ha elaborado para obtener su grado de Licenciatura en Derecho.

He revisado y he hecho las observaciones relativas al contenido analizado, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación. He verificado que se han hecho las modificaciones correspondientes a las observaciones indicadas.

Por consiguiente, este trabajo cuenta con mi aval para ser presentado en la defensa pública.
Atte.

Firma
Nombre: Andrey Esteban Morales Mejía
Cédula: 1-1391-0062
Carné: 27201

19 de julio del 2019

Señores
Comisión de Trabajos Finales de Graduación
Universidad Hispanoamericana
Escuela de Derecho

Estimados señores:

Yo Noel Molina Blanco, cédula ocho cero cuarenta y seis cero quinientos ochenta y siete, vecino de San Juan de Tibás, de profesión Licenciado en Filología clásica, y que cuento con conocimientos y experiencia en revisión filológica de textos, doy fe de haber revisado el trabajo final de graduación del sustentante Edwin Pérez Brenes, titulado, "Convenio de Budapest, y el incumplimiento de nuestro país ante la falta de regulación adecuada del ciberdelito de las personas jurídicas", para optar por el grado de Licenciatura en Derecho.

Después de la revisión y corrección de la estudiante, considero que el Informe del Trabajo Final de Graduación indicado anteriormente, cuenta con la revisión y corrección filológica en aspectos fundamentales que lo hacen apto para ser presentado al proceso de evaluación de los Trabajos Finales de Graduación en el nivel de Licenciatura.

Quedo a su disposición para cualquier consulta en:
Email: noelmolina16@hotmail.com
Teléfono celular: 84199224
Carné Colypro 57465

De ustedes muy atentamente,

Noël Molina Blanco
Carné Colypro 57465

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, agosto 5 del 2019

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito Edwin Perez Brenes con número de identificación 1-1162-0312 autor del trabajo de graduación titulado "CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAIS ANTE LA FALTA DE REGULACION ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURIDICAS", presentado y aprobado en el año 2019 como requisito para optar por el título de Licenciatura en Derecho; (SI) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Firma y Documento de Identidad

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, agosto 5 del 2019

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito Edwin Perez Brenes con número de identificación 1-1162-0312 autor del trabajo de graduación titulado "CONVENIO DE BUDAPEST, Y EL INCUMPLIMIENTO DE NUESTRO PAIS ANTE LA FALTA DE REGULACION ADECUADA DEL CIBERDELITO DE LAS PERSONAS JURIDICAS", presentado y aprobado en el año 2019 como requisito para optar por el título de Licenciatura en Derecho; (SI) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Firma y Documento de Identidad