HECHOS PUNIBLES INFORMÁTICOS Y SU REGULACIÓN EN LA LEGISLACIÓN PARAGUAYA.

Silvia María Escobar Noguera

Hugo Daniel Rivas Arévalos

Tutora: Abg. Mirta de Jesús Noguera Irala

Tesis presentada en la Universidad Tecnológica Intercontinental como requisito parcial para la obtención del título de Abogado.

Caazapá, 2021

Constancia de aprobación del tutor

Quien suscribe Abg. Mirta de Jesús Noguera Irala con documento de identidad N°4.567.803, tutora del trabajo de investigación titulado “Hechos punibles informáticos y su regulación en la legislación paraguaya”, elaborada por los alumnos Silvia María Escobar Noguera, con C.I.Nº 4.002.686 y Hugo Daniel Rivas Arévalos con C.I.Nº 3.956.364, para obtener el título de Abogado hace constar que el mismo reúne los requisitos formales y de fondo exigido por la facultad de Derecho de la Universidad Tecnológica Intercontinental y puede ser sometido a evaluación y presentarse ante los docentes que fueron designados para la conformación la Mesa Examinadora.

En la ciudad de Caazapá a los 27 días del mes de octubre de 2021

Abg. Mirta de Jesús Noguera Irala

Dedicatoria

A Dios: por su fidelidad ante la adversidad, por las alegrías, por su grandeza y misericordia.

A nuestros padres: quienes se han mantenido firmes a lado nuestro, por acompañarnos siempre en el camino que hemos decidido emprender.

A nuestro Hijo Mathias Donatto: la inspiración más grande para seguir construyendo meta juntos. Hijo nuestro logro para ti.

Agradecimiento

A la Universidad Tecnológica Intercontinental, por brindarnos la oportunidad de una formación profesional de calidad.

A los docentes de la Universidad, quienes a través de sus enseñanzas han colaborado significativamente a este proceso.

Tabla de contenido

Hechos punibles informáticos y su regulación en La Legislación Paraguaya.

Silvia María Escobar Noguera

Hugo Daniel Rivas Arévalos

Universidad Tecnológica Internacional

Carrera de Derecho, Sede Caazapá

silvim04@gmail.com

hugirivas88@gmail.com

Resumen

La investigación realizada se denomina “Hechos punibles informáticos y su regulación en la legislación paraguaya”, la misma es de enfoque cualitativo, de alcance descriptiva que buscó describir la manera que afronta Paraguay los delitos informáticos. Se ha enmarcado los hechos punibles informáticos tipificados en la legislación paraguaya, se identificó las normativas que protegen al individuo de los delitos informáticos y la sanción prevista llegando a concluir: Paraguay posee una escasa normativa en relación a este flagelo, como se ha indicado, Paraguay hace alusión a varias normativas que luchan contra los delitos informáticos, pero, no están enunciados implícitamente como tal, como lo es el caso de los derechos del autor. Paraguay se centra en pocas figuras delictivas, ignorando muchas otras que pudieran surgir de la virtualidad, uno de los elementos con el que Paraguay cuenta para luchar contra este tipo de delitos es el convenio de Budapest para prevenir las conductas que atenten contra la confidencialidad, integridad, disponibilidad de los datos y de sistemas informáticos, pero, lo más importante radica en su finalidad de establecer un marco jurídico internacional que permita impulsar la cooperación internacional. Las normativas son el Convención de Budapest, la Ley Nº 4439/11, las Resoluciones Nº 3459/10 y 4408/11, la Ley Nº. 2861/2006, La ley del comercio electrónico, Ley 1328 del Derecho del Autor y Derechos conexos. Las penalidades se encuentran estipuladas en el código penal paraguayo, estableciendo sanciones de 1 año o multa, en algunos casos 5 años, y otros como la pornografía infantil, hasta 10 años.

Palabras claves: Hechos punibles, Delitos informáticos, normativa, sanción

Marco introductorio

Planteamiento del problema de investigación

El siglo XXI trajo aparejado importantes avances en la tecnología mediante el uso de teléfonos inteligentes y el internet. Los smartphones, tablets u ordenadores hoy día son una realidad a cuyo uso el mundo entero se encuentra supeditada, de ello parte la interconexión de los individuos por medio de las redes sociales, la cual es considerada un elemento clave para la sociedad en esta era digitalizada.

De tal forma, se debe de tener en cuenta que el acceso a este mundo tecnológico tiene sus riesgos. Tal como lo enuncia Pino (2016) “El avance de la tecnología informática han surgido una serie de comportamientos disvaliosos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad”

La información personal que subimos a internet como fotos, vídeos, o las contraseñas de nuestras cuentas personales, pueden estar en riesgo si no tomamos las medidas adecuadas ante el robo de identidad o la información sensible de nuestros dispositivos.

La presente investigación se enfoca a analizar la siguiente pregunta: ¿Cómo afronta Paraguay los delitos informáticos?

Preguntas de Investigación

¿Cuáles son los hechos punibles informáticos tipificados en la legislación paraguaya?

¿Cuáles son las normativas que protegen al individuo de los delitos informáticos?

¿Cuál es la sanción prevista para los delitos informáticos?

Objetivo General

Describir la manera en que Paraguay afronta los delitos informáticos

Objetivos específicos

Conocer los hechos punibles informáticos tipificados en la legislación paraguaya

Identificar las normativas que protegen al individuo de los delitos informáticos

Identificar la sanción prevista para los delitos informáticos

Justificación

La era tecnológica ha progresado indefectiblemente, pero, nadie imaginaba la gran revolución que impondría, Con el paso del tiempo, se ha comprobado que no sólo es un nuevo canal de comunicación, sino que, además, se ha convertido en el medio a través del cual ahora se da la vida cotidiana.

La evolución de la web supone una serie de ventajas, pero también de inconvenientes, éstos son grandes peligros que puede acarrear su utilización, como la facilidad de comisión de numerosos delitos relacionados con la imagen, la economía o la propiedad intelectual, entre otros.

Esta dependencia de la Sociedad de la Información a las nuevas tecnologías de la información y de las comunicaciones (TIC), hace patente el grave daño que los llamados delitos informáticos o la delincuencia informática pueden causar a nuestro nuevo estilo de vida, la importancia que cobra la seguridad con la que han de contar los equipos informáticos y las redes telemáticas con el fin de poner obstáculos y luchar con dichas conductas delictivas, y la necesidad de tipificar y reformar determinadas conductas, a fin de que esta sean efectiva y positivamente perseguidas y castigadas en el ámbito penal. (Pino, 2016, pág. 6)

La investigación se reduce a analizar los hechos punibles informáticos tipificados en la legislación paraguaya. Se determinará conceptos, criterios y legislaciones vigentes en el Derecho positivo Nacional y las bases jurídicas, se pretende enriquecer conocimientos sobre el tema abordado, cuyo contenido es vital y de mucha persecución en la actualidad.

El estudio a realizar se podrá llevar a cabo por contar con todos los recursos necesarios, ya sea económico, humano, bibliográfico y de tiempo, que será de utilidad a Abogados en ejercicio de la profesión, futuros abogados y a aquellas personas que tiene tienen interés en el tema.

Viabilidad

La investigación realizada es viable por contar con los materiales necesarios, fuentes de informaciones relevantes para cumplir con los objetivos y responder las preguntas de investigación.

Los recursos financieros serán costeados en su totalidad por el autor del proyecto de investigación.

Así mismo los recursos humanos que aportarán informaciones y conocimientos para elaboración del mismo.

Marco Teórico

Antecedentes de la investigación

En el plano internacional se puede mencionar una numerosa cantidad de investigaciones, en Colombia, Jorge Eliécer Ojeda Pérez, Miguel Eugenio Arias Flórez, Fernando Rincón Rodríguez y Libardo Alberto Daza Martínez, en el año 2010, se abocaron a indagar sobre los Delitos informáticos y entorno jurídico vigente en Colombia confirmando que su investigación describe y analiza la evolución y el marco conceptual de los delitos informáticos planteados por diferentes autores nacionales e internacionales, y establece la relación con la reciente Ley 1273 de 2009, mediante la cual la legislación colombiana se equipara con la de otros países en cuanto a la normatividad sobre el cibercrimen, que ha venido vulnerando distintos campos de las relaciones y comunicaciones personales, empresariales e institucionales. El ciberdelito, como tendencia que incide no sólo en el campo tecnológico sino también en el económico, político y social, debe ser conocido, evaluado y enfrentado, por lo cual el análisis de la norma, su aporte y alcance puede dar otros elementos de juicio para entender la realidad de nuestras organizaciones y visualizar sus políticas y estrategias, a la luz de la misma norma y de los estándares mundiales sobre seguridad informática. (Ojeda Perez, Arias Flórez, Ricon Rodriguez, & Daza Martinez , 2010)

En el año 2016 en Ecuador, Dr. Santiago Acurio Del Pino, Profesor de Derecho Informático de la PUCE, realizaba una investigación denominada “Delitos Informáticos: Generalidades” donde determina que los delitos informáticos, son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, pero a pesar de eso y de no contar ni con una policía entrenada para investigar dichos hechos, ni un Ministerio Público que pueda dar las directrices para la correcta indagación de dichos actos delictivos, por no contar entre otras con una Unidad Especial para la investigación y persecución de estas infracciones informáticas, existen dos problemas principales que a continuación se exponen: “La concepción tradicional de tiempo y espacio y el anonimato del Sujeto Activo”. al. (Pino, 2016)

En el año 2017 en chile, Laura Mayer Lux con la investigación “El Bien Jurídico Protegido En Los Delitos Informáticos” en la que asume que los delitos informáticos tutelan

un bien jurídico específico, propiamente informático. Sobre esa base, plantea que reconocer un interés de esas características se justifica si dichos delitos, además de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. Para definir su bien jurídico, el estudio reflexiona sobre las funciones que cumplen los sistemas informáticos para el libre desarrollo de la persona y las instituciones que están a su servicio en un Estado democrático de derecho. (Lux, El bien juridico protegido en los delitos informaticos, 2017)

La misma autora, Laura Mayer en el año 2018 realiza otra investigación sobre los Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos, en donde examina algunos elementos criminológicos que pueden contribuir al análisis jurídico/penal de los delitos informáticos. El estudio se centra en los delitos que inciden en el soporte lógico de un sistema informático e implican el uso de redes computacionales, distinguiendo medios y contextos de comisión, sujetos y consecuencias. (Lux, Elementos criminológicos para el análisis jurídico/penal, 2018)

En el Paraguay los Delitos informáticos tomaron notoriedad desde el año 2010, la investigación en relación al tema aún no se ha desarrollado a profundidad, en el año 2018, la Unidad Especializada de Delitos Informáticos ha realizado una investigación aportando datos específicos a la Ciudadanía sobre los delitos informáticos en las redes sociales.

Así mismo, La Abogada Fátima Girala, egresada de la Universidad Nacional de Asunción, Notaria y Escribana Pública, Magister en Ciencias Penales por la Universidad Nacional de Asunción, Docente de la Universidad de Integración de las Américas y Egresada de la Escuela Judicial del Paraguay en el año 2020, ha desarrollado una investigación denominada “El mundo, la tecnología y los Delitos Informáticos en el Paraguay”, en ella expresa: “El término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet, todas estas conceptuaciones son aproximaciones a lo que son los delitos informáticos. En fin, el avance de la tecnología ha generado que el derecho pueda tipificar sobre ciertas conductas a fin de evitar daños a la información, a los sistemas, a la confidencialidad entre otros. En tal sentido existen numerosos países que han introducido a través de leyes particulares o en sus leyes penales a los Delitos Informáticos. Nuestro país tiene incorporada en la reforma al Código Penal algunas figuras cometidas por medios informáticos como la interceptación de datos, el acceso a sistemas no autorizados entre otros.

Actualmente, se encuentran en tratamientos otras leyes que ayuden a complementar las ya existentes para ser incorporadas al código penal y falta sin lugar a dudas la tipificación de otros delitos que ayuden a llenar las lagunas existentes". (Girala, 2020)

Al indagar profundamente sobre investigaciones anteriores, se determina el escaso material de escritura nacional, la mayor parte de las investigaciones son de carácter internacional, enfocando así la atención sobre la necesidad de inquirir conocimientos sobre el tema a abordar.

Evolución Histórica

A lo largo de la historia el hombre, ante la necesidad de comunicarse, transmitir y tratar información, ha elaborado diferentes sistemas a tales fines que van desde las señales de humo, código morse, teléfono hasta llegar a la informática que es la ciencia encargada del estudio y desarrollo de máquinas para, al menos inicialmente ayudar al hombre con trabajos rutinarios y repetitivos; con el tiempo se fue diversificando su uso. Luego nace Internet como tecnología que pondría cultura, ciencia e información al alcance de millones de personas en todo el mundo. Si bien este adelanto tiene innumerables ventajas de las que muchos usuarios y empresas han logrado extraer importantes beneficios, también abre las puertas a conductas antisociales y delictivas ofreciendo oportunidades nuevas y complejas de infringir la ley. Un cambio social ha operado en las últimas décadas, que resulta íntimamente vinculado a la evolución tecnológica operada en ese transcurso de tiempo, generándose problemas para la protección de intereses sociales no convencionales y para la represión de las conductas delictivas realizadas a través de medios no convencionales, en este contexto debe de tenerse en cuenta que el impacto de la explosión tecnológica es un problema de política criminal que se conoce sobradamente. (Ceresole & Oyarzábal, 2014)

La revolución en este sector ha sido tal que ha cambiado la forma del hombre de relacionarse con el mundo y las personas que le rodean. Un cambio tan grande que nadie hubiera podido preverlo jamás. No en vano el acontecimiento ha sido llamado por algunos como "Tercera Revolución Industrial" o incluso "Revolución de la Inteligencia", haciendo uso ésta última, a mi juicio, de vocablos totalmente inapropiados para su denominación. Es la aparición de las llamadas TIC's (Tecnologías de la Información y Comunicación) pero, sobre todo, su masificación, el elemento que mejor define la nueva era

que nos ha tocado vivir. Lo cierto es que esta tecnología representa, desde mi punto de vista, un salto cualitativo mayor aún que el descubrimiento de la electricidad. Técnicamente, se consideran Tecnologías de la Información y Comunicación tanto al conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, como al conjunto de procesos y productos derivados de las nuevas herramientas (hardware y software)1. Se trata de instrumentos que nos permiten estar informados prácticamente al instante de lo que ocurre en el mundo, comunicarnos en menos de un segundo con cualquier persona de La Tierra. Por eso ahora pueden comprenderse mis palabras anteriores relacionadas con la monumental evolución que esto ha supuesto. (Gomez, 2010)

Vivimos en un mundo que cambia rápidamente. Antes, podíamos tener la certeza de que nadie podía acceder a información sobre nuestras vidas privadas. La información era solo una forma de llevar registros. Ese tiempo ha pasado, y con él, lo que podemos llamar intimidad. La información sobre nuestra vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema, que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más y más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularlos. Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la “era de la información”2 , a lo que con más propiedad, podríamos decir que más bien estamos frente a la “era de la informática”. (Pino, 2016)

La evolución en el manejo, potencia y versatilidad del software-equipos informáticos ha sido tan rápida que antes se podía tener la entera certeza que nadie era capaz de hurtar información personal, sin embargo esto es pasado, debido a la globalización de los procesos la explosión de las industrias computacionales e informáticas ha permitido la creación de un sistema, que puede guardar grandes cantidades de información y transmitirla en muy poco tiempo, cada vez más personas acceden a dichos contenidos,

sin que las legislaciones sean capaces de regularlos. (Gonzalez, Bermeo, Villacreses, & Guerrero, 2018)

El desarrollo y el impacto de las Tecnologías de la Información y las Comunicaciones (TIC) han generado la concomitante necesidad de ajuste de muchas de las formas de operación y de gestión de las organizaciones, tanto de los procedimientos y estándares de las ciencias y otras tecnologías, como de la interpretación del mundo, sus culturas y paradigmas; y de esa tendencia no se excluye el Derecho. La información hace parte del proceso de bienes que llegan a ser universalmente reconocidos y como tales deben ser jurídicamente protegidos, junto a las herramientas que facilitan su manejo. (Ojeda Perez, Arias Flórez, Ricon Rodriguez, & Daza Martinez , 2010)

Los progresos tecnológicos a nivel mundial, así como el incremento de la capacidad de almacenamiento que tienen los equipos electrónicos en la actualidad, hacen más difíciles las tareas de control, es muy difícil legislar tal cantidad de dispositivos a la par con la conducta de sus usuarios que además están influenciados por las presiones sociales que incitan a las masas a buscar nuevas formas de obtener dinero, bajo este contexto abordar el estudio que tienen las actividades informáticas en delitos, resulta un asunto complejo para quien busca determinar el impacto de las nuevas tecnologías en los entornos sociales. Es decir, el desarrollo y la masificación de las nuevas tecnologías en la informática, han contribuido a los estudios que en ámbito jurídico buscan regular estas actividades con la meta de crear accionantes legales por medio del debido proceso den solución a conflictos enmarcados en el contexto descrito anteriormente. Resulta importante analizar que de forma paralela a los avances tecnológicos y la influencia que se ha ejercido en el entorno de las personas, se han terminado llevando a cabo comportamientos delincuenciales, que antes no eran posibles de imaginar y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad. (Gonzalez, Bermeo, Villacreses, & Guerrero, 2018)

Delitos informáticos

El Delito informático es aquel que se da con la ayuda de la informática o de técnicas anexas; es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o

vulnerando los derechos del titular de un elemento informático, ya sea hardware o software. (Pino, 2016)

El delito informático en forma típica y atípica, entendiendo por la primera a las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin y por las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. (Valdez, 2000)

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas, y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático. (Alcívar Trejo, Domenech Alvarez, & Ortìz Chimbo, 2015)

A medida que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático y pornografía infantil, entre otros. Para enfrentarlos, no obstante, la dificultad para descubrirlos, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos. (Ojeda Perez, Arias Flórez, Ricon Rodriguez, & Daza Martinez , 2010)

El ciberdelito, al igual que otras figuras penales, ha sido objeto de análisis por parte de juristas y expertos en seguridad informática de todo el mundo; lo que permitió que muchas legislaciones del continente americano tipifiquen conductas ciber delictuales, tomando en consideración lo que se ha analizado doctrinalmente y tipificado en otros continentes. (Narváez Montenegro & Recalde Machado, 2018)

Sin embargo, no ha existido un estudio adecuado sobre la realidad del delito informático en el continente americano que haya permitido identificar los imperfectos jurídicos respecto a ciertas ciber conductas que deben ser consideradas y sancionadas como figuras penales independientes, lo que llevó a la necesidad de efectuar una investigación que identifique los delitos informáticos tipificados en países que más avances presentan sobre el tema, y, en base a ello, se estableció las falencias y/o vacíos presentes en las legislaciones del continente americano. Este trabajo de investigación se fundamentó en publicaciones nacidas en la Academia y del análisis que al respecto efectuaron los autores, aplicando métodos teóricos y empíricos que, conjugados con la técnica de la entrevista y la encuesta, concluyó en una propuesta viable y novedosa. (Narváez Montenegro & Recalde Machado, 2018)

De esta forma se detalló las conductas criminales ejecutadas con herramientas informáticas que constan en la legislación americana; y una vez identificadas se detectó las falencias existentes y se proporcionó una posible solución en base a la tipificación de ciertas ciber-conductas que no constan como figuras penales independientes en los cuerpos jurídico-penales de América, y que en muchas ocasiones son sancionadas acoplándolas a figuras penales tradicionales que contienen una pena no proporcional con el daño causado. (Narváez Montenegro & Recalde Machado, 2018)

El delito informático ha sido objeto de análisis y por parte de juristas y expertos en seguridad informática; en base a estos estudios muchas legislaciones del mundo han tipificado varias conductas como cibercrímenes. Sin embargo, no existe una clasificación única del delito informático, lo que ha generado que cada legislación le otorgue un tratamiento diferente, no solo en cuanto a la sanción, si no a la forma de consideración de cada uno de ellos: tanto en las circunstancias de cómo es cometido, como en la forma de investigarlo y procesarlo. (Montenegro, 2015)

Las herramientas de los ciberdelincuentes han evolucionado si no más rápido, por lo menos paralelamente al desarrollo tecnológico, como ha venido sucediendo con los virus informáticos. En un comienzo, los ciberdelincuentes infectaban los equipos de sus víctimas al transportar mano a mano los virus desarrollados, en los medios de almacenamiento de información disponibles en ese momento: los disquetes. Más tarde, utilizaron las redes de datos al aprovechar la internet, pero encontraron la barrera de las restricciones de acceso para evitar contagios. De nuevo, regresaron a la difusión contaminante mano a mano al emplear

las memorias móviles con puerto USB y arreciaron los bombardeos de malware1 en la internet. De igual manera, los ciberdelincuentes han utilizado el correo electrónico y los chats rooms o salas de conversación virtual de internet para buscar presas vulnerables. (Ojeda Perez, Arias Flórez, Ricon Rodriguez, & Daza Martinez , 2010)

Los delitos informáticos en países sudamericanos

Argentina. Este país se sumó a diversas legislaciones del mundo que tipifican conductas cibercriminales, cuando el 4 de junio del 2008 sancionó la Ley 26.388, República de Argentina (2008) que reforma los artículos 77, 128, 153, 155, 157, 173, 183,197 y el epígrafe del Capítulo III, del Título V, del Libro II, además que se derogan el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal, incluyendo las siguientes conductas cibercriminales: Interrupción de comunicaciones, daño informático agravado, distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus. Esta normativa sienta la base legal para que los jueces puedan sancionar conductas delictuales que las encuadraban en un tipo de adaptación jurídica- en un delito ya tipificado. (Montenegro, 2015)

Brasil. En este Estado, el debate sobre la situación jurídica del delito informático no ha estado a la par de su auge tecnológico y económico. Mientras otras legislaciones con menor desarrollo estipularon una normativa que tipifica y sanciona esta clase de delitos, Brasil tenía que a adaptar las conductas cibercriminales a figuras penales tradicionales ya tipificadas. Tuvo que acontecer un hecho que conmocionó considerablemente la sociedad brasileña para que el gobierno tome en serio el debate y la necesidad de crear una ley que tipifique con más amplitud este tipo de delitos. Éste fue el acaecido a la conocida actriz brasileña Carolina Dieckmann, cuyas fotos fueron publicadas en internet por un sitio especializado en celebridades Egotastic, sin su autorización. Lo acontecido a Dieckmann hizo que la autoridad ejecutiva y legislativa tome medidas jurídicas urgentes que protejan a la población de este tipo de ataques, llevando a la presidenta de Brasil, Ec. Dilma Rousseff, a firmar dos leyes que reforman el Código Penal, tipificando y sancionando varios delitos electrónicos. El proyecto fue aprobado por la Cámara de Representantes el 7 de noviembre del 2012; y en el que se tipifican los siguientes:

- El acceso no autorizado a ordenadores, conectados o no a internet, mediante la violación de sus mecanismos de seguridad

- El robo de contraseñas y contenidos de correos electrónicos o

- Hacer caer intencionalmente un Website

- La invasión de dispositivos electrónicos ajenos con el fin de obtener, cambiar o destruir datos o informaciones.

- La producción y distribución de dispositivos que permitan invadir teléfonos inteligentes o tabletas electrónicas.

- La obtención ilegal de datos bancarios por vías electrónicas

La normativa también amplía a los medios electrónicos la prohibición de contenidos racistas. Una de las falencias que expertos en seguridad informática y juristas han detectado en esta Ley, es la falta de precisión en los términos que se emplea en la misma: de acuerdo con la ley, incurre en delito la persona que accede a un ordenador superando un mecanismo de seguridad, sin embargo, no especifica lo que se considera un mecanismo de seguridad. (Montenegro, 2015)

Bolivia. Se sanciona la violación de la correspondencia electrónica privada y la falsificación y suplantación de identidad en la web; manipulación informática, la alternación, acceso y uso indebido de datos informáticos; falsedad y falsificación de documentos privados en un sistema digital. Es necesario indicar que antes de la expedición de esta ley la falsedad y falsificación se aplicaba únicamente a documentos físicos o impresos; delitos contra la propiedad intelectual de las obras con soporte electrónico en la web. Se sanciona a quien cometa sabotaje informático e impida el normal funcionamiento del sistema de información o telecomunicaciones. (Narváez Montenegro & Recalde Machado, 2018)

Venezuela. Se puede revelar que, en cuanto a delitos informáticos, la legislación venezolana es de las más completas del continente americano. Los cibercrímenes tipificados son: Acceso indebido; sabotaje o daño a sistemas; acceso indebido o sabotaje a sistemas protegidos; posesión de equipos o prestación de servicios de sabotaje; espionaje informático; falsificación de documentos; hurto informático; fraude informático; obtención indebida de

bienes o servicios; manejo fraudulento de tarjetas inteligentes o instrumentos análogos; apropiación de tarjetas inteligentes o instrumentos análogos; provisión indebida de bienes o servicios, posesión de equipo para falsificaciones; violación de la privacidad de la data o información de carácter personal; violación de la privacidad de las comunicaciones; revelación indebida de data o información de carácter personal; difusión o exhibición de material pornográfico; exhibición pornográfica de niños o adolescentes; apropiación de propiedad intelectual y oferta engañosa. (Narváez Montenegro & Recalde Machado, 2018)

Chile. El 7 de julio de 1993, Latinoamérica empezó a incluir en su normativa a los delitos informáticos. Chile fue de los primeros Estados en crear una ley que tipificó estos delitos, mediante la Ley 19223 denominada "Ley contra Delitos Informáticos", (República de Chile, 1993). Esta ley ofreció en aquella época un aporte significativo en cuanto al bien jurídico que es protegido por la tipificación de los Delitos Informáticos. Aunque no se trata de un cuerpo jurídico completo -para la actualidad. Este cuerpo jurídico está compuesto por cuatro artículos que tratan sobre la destrucción o inutilización de un sistema de tratamiento de información. Hecho que puede ser castigado con prisión de un año y medio a cinco. Igualmente se tipifica el apoderamiento, uso o conocimiento indebido, intercepción, interferencia o accesión indebida en un sistema de información.

Es menester destacar que Chile fue de los pioneros no solo en la tipificación de los delitos informáticos, sino en crear entes que se encarguen de su investigación. Efectivamente, el 16 de octubre del año 2000 se crea la Unidad especializada en delitos cometidos vía Internet. Este ente forma parte de La Policía de investigaciones de Chile, y se encarga de detectar amenazas, estafas, falsificación, pornografía infantil en internet, y todo tipo de conducta informática que lesione derechos de terceros. Sin embargo, de lo efectuado por la Comunidad Internacional, existen criterios que manifiestan que las clasificaciones propuestas resultan incompletas frente a la gran cantidad de conductas cibercriminales que se presentan en el diario vivir de las personas, siendo menester detectar las debilidades detectadas en las clasificaciones planteadas por organismos internacionales y las legislaciones. (Montenegro, 2015)

Colombia. Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos., daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios

web para capturar datos personales -es primordial mencionar que este artículo tipifica lo que comúnmente se denomina phishing-, hurto por medios informáticos y semejantes, transferencia no consentida de activo. (Narváez Montenegro & Recalde Machado, 2018)

Perú. En los delitos contra datos y sistemas informáticos se contempla: el acceso ilícito, atentado contra la integridad de datos informáticos, y el atentado contra la integridad de sistemas informático. En los delitos informáticos contra la indemnidad y libertades sexuales se contempla: proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. En los delitos contra la intimidad y el secreto de las comunicaciones se contempla: tráfico ilegal de datos, interceptación de datos informáticos. En los delitos informáticos contra el patrimonio se contempla: fraudes informáticos. En los delitos informáticos contra la fe pública: suplantación de identidad. (Narváez Montenegro & Recalde Machado, 2018)

Uruguay. Uno de los países cuya legislación penal se encuentra más rezagada en materia de delitos informáticos es la uruguaya. En la actualidad la temática del presente artículo está amparada por la ley No 18.331 de Protección de Datos Personales y Acción de Habeas Data y por los artículos 72 y 332 de la Constitución. Sin embargo, el Parlamento uruguayo, en vista del alto índice de delitos que se dan empleando medios informáticos, discute una reforma del Código del Proceso Penal donde se incluye un capítulo relativo a los delitos informáticos, entre los que se consideran: acceso ilícito a sistemas informáticos; intercepción ilícita de información; ataques a la integridad de los datos y del sistema; uso indebido de dispositivos, software o claves de acceso; falsificación y fraude informático. (Narváez Montenegro & Recalde Machado, 2018)

Los delitos informáticos en el Paraguay

La llegada a del avance tecnológico a Paraguay significo un cambio significativo, pues a partir de esto, comienzan a surgir nuevos horizontes para muchas personas, como también la aparición de grandes empresas internacionales, que vieron el potencial de la implementación real de esta red de comunicación en la Republica, por supuesto, comenzó con los sistemas de telefonía celular, para luego convertirse hoy, justamente a través de los teléfonos móviles, en una fuente de información y comunicación, antes inimaginables. (Girala, 2020)

La influencia en Paraguay es muy grande, tanto que hoy la penetración de internet es muy importante, pues la misma se da a través de los sistemas de telefonía móvil, por lo que hay que analizar el porcentaje de personas con telefonía móvil, para saber cuánto de penetración de internet hay en Paraguay (y no las computadoras portátiles o estáticas) que hoy están en constante tendencia de aumento. (Girala, 2020)

Conforme a los expuesto, se vio la necesidad de que la aplicación de la tecnología estuviera protegido, y como se vive en un Estado Social de Derecho, el modo de hacerlo es a través de la acción del Estado, pero como este tampoco puede usar la fuerza por usarlo, establece un sistema normativo, para que una vez transgredido este, pueda aplicar las sanciones previstas en aquellas. Tal es así que, para la utilización de internet, se estableció un sistema de reglas, y hoy existe un sistema normativo al respecto en la Republica.

La fiscalía general de la Republica del Paraguay, define a los delitos informáticos como los delitos informáticos son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas. (Ministerio Publico. Republica del Paraguay, 2018)

La Unidad Especializada de Delitos Informáticos, fue creada para combatir los hechos punibles cometidos a través de la tecnología. La Unidad investiga el acceso indebido a sistemas informáticos, sabotaje de sistemas informáticos; estafa mediante sistemas informáticos, falsificación de tarjetas de débito o crédito, entre otros. (Unidad Especializada de Delitos Informáticos, 2018)

En el Paraguay se tienen en consideración en el Código Penal y en el Código Procesal Penal, aunque algunas no directamente como delitos informáticos, los siguientes actos: Lesión del derecho a la comunicación y a la imagen , Violación del secreto de la comunicación, Alteración de datos Sabotaje de computadoras, Operaciones fraudulentas por computadora, Aprovechamiento clandestino de una prestación, Perturbación de instalaciones de telecomunicaciones, Pornografía infantil Intercepción, secuestro, apertura y examen de correspondencia, Intervención de comunicaciones, Derechos de Autor. (Centurión, 2010)

Existen diversas leyes y artículos que sancionan los delitos informáticos planteados en la sección anterior, que buscan regular las actividades que hacen uso de las tecnologías y las comunicaciones para fines maliciosos o dañinos. (Centurión, 2010)

Paraguay también existen leyes que sancionan delitos cometidos a través de sistemas informáticos, incluso, a partir del 1 de octubre de 2010, entró en funcionamiento la Unidad de Delitos Informáticos que actualmente se encuentra a cargo del fiscal Abog. Fiscal Ariel Martínez, junto al fiscal adjunto Fiscal adjunto Abg. Fiscal María Teresa Aguirre. Sepa cuáles son los artículos que reglamentan los diferentes tipos de delitos informáticos. (Proteccion Online.com, 2012)

A modo de resumen, el departamento de cooperación jurídica presenta una recopilación de 6 artículos que reglamentan y sancionan algunas prácticas delictivas referentes a delitos informáticos que forman parte del código penal paraguayo que refiere a hechos relacionados con pornografía infantil, intercepción ilícita, interferencia en el sistema, interferencia de datos, fraude informático e intercepción ilícita. A continuación, las disposiciones específicas con sus respectivos delineamientos. (Proteccion Online.com, 2012)

Entonces, al hablar de seguridad en Internet nos estamos refiriendo a la gestión de claves, confidencialidad, imposibilidad de repudio, integridad, autenticación y autorización. Ahora bien, al hablar de vulnerabilidades o pérdidas de acceso, uso indebido de datos, clonación de tarjetas, nos estamos refiriendo a un nuevo universo de hechos punibles que en la mayoría de los casos ya se encontraban legislados en nuestro Código Penal, siendo ampliados en el año 2011, por la Ley Nro. 4439 modificatoria. (Girala, 2020)

Los tipos de delitos informáticos

La tecnología aplicada en el Ciberespacio ha modificado por completo las diversas relaciones sociales y la globalización ha puesto en jaque a los pilares del Estado y las bases de la sociedad tradicional, hasta el punto de crear “una sociedad” paralela a la física. Este punto de inflexión ha generado grandes avances del ser humano como la comunicación y acceso al conocimiento entre millones de personas a nivel mundial. No obstante, este espacio cibernético no está exento de problemas: está habitado también por grupos extremistas, terroristas, delincuentes e individuos sin fines pacíficos. Esto conlleva nuevos planteamientos

de regulación, de forma urgente y necesaria para abordar esta problemática, puesto que, si un delito se comete utilizando tecnología y genera impactos en diversos territorios. (Sequera & Samaniego, 2018)

Según las Resoluciones Nº 3459/10 y 4408/11, los tipos penales de competencia exclusiva de la Unidad Especializada en Delitos Informáticos son los siguientes: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos. (Unidad Especializada de Delitos Informáticos, 2018)

Preparación de acceso indebido e intercepción de datos.

En el caso del 146d, se trata adelantar la punición de actos preparatorios correspondientes a los dos artículos anteriores. En tal sentido, se castigará tanto la producción, la difusión o hacer accesible a terceros claves de acceso u otros códigos de seguridad, así como programas de computación destinados a la realización de las conductas señaladas en los arts. 146b y 146c. Merece especial atención la cuestión de los programas informáticos que sirven para eludir las medidas de seguridad. Esto debido a que en muchas empresas se suelen utilizar ese tipo de programas para probar justamente si su sistema es seguro o no.

En Alemania, una empresa que prestaba servicios de seguridad informática, un profesor de la Universidad Técnica de Berlín y un usuario de este tipo de programas, habían solicitado al Tribunal Constitucional de aquel país, una declaración de inconstitucionalidad del inciso 1°, apartado 2 del 202c del StGB (fuente directa de nuestro 146d, inc. 1°, num. 2). El Tribunal Constitucional alemán rechazó las acciones planteadas, basado en considerar que no había habido violación de los derechos constitucionales. Según el tribunal, la legislación solo se aplica a los programas desarrollados con la intención ilegal. Es decir, aquellos programas que son creados con una intención lícita no pueden ser abarcados por el tipo penal, aunque por su utilización pueda dársele un destino ilícito. Nótese por tanto, que la característica definitoria para considerar la conducta como cumpliendo con los presupuestos del tipo penal, es la intención del sujeto. (Preda, 2012)

Acceso indebido a datos. Este hecho punible cubre una laguna de punibilidad del fenómeno denominado hacking y que afecta el ámbito de la inviolabilidad del ámbito de vida y la intimidad de un individuo. Dicho de una manera más sencilla, el Acceso indebido de datos sería una versión electrónica de la Violación de domicilio prevista en el art. 141 del CP, tal como lo concibe Sieber. Su tipificación igualmente se adapta a la recomendación del art. 2 del Convenio de Budapest del 2001. (Preda, 2012)

En el inc. 1 se advierte la formulación de la conducta prohibida, que cosiste simplemente en acceder a datos no destinados al autor o igualmente hacerle accesible esos datos a un tercero, sin autorización y violando sistemas de seguridad. Los datos deben estar protegidos justamente contra ese acceso indebido.

Por ejemplo, si un sujeto ingresa a revisar mi cuenta vía internet, debido a que logro descifrar mi contraseña de ingreso, sería una conducta que podría subsumirse ya en el art. 146b, inc. 1°, primera variante. Ahora bien, en caso que el sujeto, luego del acceso indebido a mi cuenta, realice una operación que menoscabe mi patrimonio, ya entrará en consideración el art. 188, inc. 1° del CP, num. 311 o si luego cambiara mi contraseña por una desconocida para mí, impidiéndome por tanto el acceso a mi cuenta bancaria vía internet, entonces sería de aplicación el art. 174, inc. 1°, cuarta variante. En cuanto al tipo subjetivo del Acceso indebido a datos previsto en el art. 146b, se debe apuntar que solo se castiga la conducta dolosa, aunque es suficiente el dolo eventual. El marco penal es de hasta tres años de pena privativa de libertad o multa. (Preda, 2012)

Procedimiento contra acceso indebido a datos. En prosecución a una denuncia por acceso indebido a datos, en fecha 07/10/2016, la División Especializada Contra Delitos Informáticos, procedió al allanamiento del recinto privado ubicado en la Avda. Eusebio Ayala Nº 4599 de la Ciudad de Asunción, encabezado por la Agente Fiscal de la Unidad Penal Nº 2, Especializada en Delitos Informáticos, Abg. Irma Concepción Llano, con apoyo de personal técnico de la División Especializada Contra Delitos Informáticos, del Departamento Contra Delitos Económicos de la Policía Nacional, donde se conversó con el Señor H.J.G.G, paraguayo, soltero, 35 años de edad, empleado, Técnico encargado de la Sección Informática y posteriormente se procede al registro del lugar, incautándose como evidencia Una Notebook de la marca Toshiba y un Pendrive. Las evidencias levantadas del

lugar, fueron trasladadas a cargo de la Agente Fiscal interviniente. (Direccion contra Hechos Punibles econimicos y financieros de la Policia Nacional, 2016)

Intercepción de datos. El artículo 146 c de interceptación de datos, tiene como fuente al Código Penal alemán: Será castigado con pena privativa de libertad de hasta dos años o con multa, cuando el hecho no es castigado con una pena mayor por otro precepto, quien empleando medios técnicos acceda o facilite indebidamente el acceso a datos que no están destinados a él (202a), que provienen de una transmisión no pública o de la emisión electromagnética de un sistema de procesamiento de datos. Dicho de manera más sencilla lo que busca castigar es la obtención a través de medios técnicos, datos no autorizados, datos que provengan de una transmisión privada de datos o de la emisión electromagnética de un sistema de procesamiento de datos. A su vez, el artículo contiene una cláusula de subsidiariedad. Así, por ejemplo, si una conducta concreta se subsume en uno de los tipos penales del 146c, así como en uno de los del 146b, será aplicable solo este último, pues tiene un marco penal mayor. (Girala, 2020)

Es también incluido el artículo 146 d que castiga tanto la producción, la difusión o hacer accesible a terceros claves de acceso u otros códigos de seguridad, así como programas de computación destinados a la realización de las conductas señaladas en los arts. 146b y 146c. Es aquí donde ocurre algo muy paradójico, ya que es usual que muchas empresas utilicen programas informáticos que sirven para eludir las medidas de seguridad, dichas empresas lo hacen para comprobar la seguridad de su sistema interno. (Girala, 2020)

Alteración de datos y Sabotaje a sistemas informáticos. Diccionario Panhispánico del español jurídico (2020) expone: Delito consistente en acceder, dañar, deteriorar, borrar, suprimir, modificar o inutilizar los datos registrados en una computadora o dispositivo de almacenamiento informático externo.

El art. 175 Sabotaje de computadoras pasa a denominarse Sabotaje de sistemas informáticos. También se amplía el alcance del tipo, al eliminar el requerimiento de que los datos sean de importancia vital e incluyéndose a los "particulares" como posible objeto del ataque. Anteriormente, el tipo objetivo era más restringido, en cuanto a que exigía que el procesamiento de datos sea de importancia vital. Con la reforma, basta obstaculizar un procesamiento de datos, sea o no importante para el titular. (Preda, 2012)

La modificación se aparta de la fuente alemana de nuestro art. 175 y carece de un fundamento político-criminal, pues desde la vigencia del Código Penal, nadie ha advertido que debido al requerimiento importancia vital alguna conducta no pueda ser castigada, al menos por otros artículos. Por ejemplo, el art. 174 Alteración de datos o algún delito común como el Daño o el Hurto. Estos últimos, siempre y cuando nos refiramos a los soportes de los datos, como podrían ser el disco duro o un DVD, pues solo ellos serían considerados cosas a los fines de nuestro Código Penal. (Preda, 2012)

Conductas dirigidas a causar daños físicos. El primer grupo comprende todo tipo de conductas destinadas a la destrucción física del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño. (Centurión, 2010)

Conductas dirigidas a causar daños lógicos. El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático. Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se está trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo. (Centurión, 2010)

Falsificación de tarjetas de crédito y débito. La última incorporación introducida por la Ley 4439 al Código Penal es el art. 248b Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago, cuya fuente es el 152 a del StGB. La misma se encuentra dentro del Capítulo de los hechos punibles contra la prueba documental. El artículo contiene cinco incisos. (Preda, 2012)

El 4° y el 5° definen tarjeta de crédito y medios electrónicos de pago, respectivamente. Mientras que el inciso 1°, divido en dos numerales, contiene seis conductas, las cuales si son combinadas con los diversos objetos (tarjetas de crédito u otro medio

electrónico de pago) totalizan doce tipos penales. Es así que se castiga tanto las conductas de falsificar o alterar una tarjeta de crédito u otro medio de pago electrónico, así como la de adquirirla, ofrecerla, entregarla o utilizarla. En cuanto al aspecto subjetivo, los tipos penales requieren que se actúe con dolo (ver arts. 248b inc. 1° y 17, inc.1°, ambos del CP). Además, es necesario un elemento subjetivo adicional al dolo, que en este caso es la intención de inducir al error en las relaciones jurídicas. Pero resulta importante aclarar una cuestión: no hace falta que efectivamente se induzca al error, solo se requiere que al momento de realizar una de las conductas descriptas el autor tenga por finalidad engañar. (Preda, 2012)

Estafa mediante sistemas informáticos. Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas. Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. (Centurión, 2010)

El anterior Operaciones Fraudulentas por computadora rebautizada como estafa mediante sistemas informáticos. También se reformulan los términos en los que se anuncian las cualidades de midas en los numerales del inc. 1 aunque se debe aclarar que la interpretación de los tipos penales hay contenidos no se alteran. (Preda, 2012)

Sin embargo, la modificación más significativa consiste en la inclusión de un inc.3 en el cual se prevé el castigo de conductas consistentes en autos preparatorios de tipos penales señaladas en el inc. 1. Por último, se adiciona un inciso 4 vinculado estrechamente a la anterior, pues prevé casos en los cuales se elimina la punibilidad si se colabora en evitar que los actos preparatorios se consumen. (Preda, 2012)

Prevención Contra el Ciberbulling y el Peligro en las Redes Sociales

Diseñar y promover una cultura del buen uso de la red, donde los ciudadanos adquieran conciencia de que los riesgos son reales y que es necesario aprender a reducirlos o evitarlos. La mejor respuesta para luchar contra el cibercrimen es la prevención, y ésta se

obtiene educando e incentivando a los ciudadanos a involucrarse activamente en el compromiso de salvaguardarse en la red. (Sequera & Samaniego, 2018)

Actualmente se realizan charlas en instituciones educativas de todo el país en el marco del programa Fiscalía en la Escuela. Funcionarios de la Unidad brindan capacitaciones sobre el ciberbulling, sexting, pornografía infantil y grooming, es decir, sobre los peligros y amenazas existentes contra los menores en internet. (Unidad Especializada de Delitos Informáticos, 2018)

Para el efecto, existen normativas preestablecidas que advierten la antijuridicidad de actos en relación a la manipulación de la informativa, que se encuentra establecida en las siguientes normativas que regula los delitos informáticos:

Constitución Nacional. La Constitución Nacional del Paraguay se pronuncia en relación a la privacidad de las personas:

Artículo 33. Derecho a la Intimidad - “La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas”.

Artículo 36. Inviolabilidad del patrimonio documental y de la comunicación privada: “El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación a lo prescripto anteriormente carecen de valor en juicio.

En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado".

Artículo 23. De la prueba de la verdad: "La prueba de la verdad y de la notoriedad no serán admisibles en los procesos que se promoviesen con motivo de publicaciones de cualquier carácter que afecten al honor, a la reputación o a la dignidad de las personas, y que se refieran a delitos de acción penal privada o a conductas privadas que esta Constitución o la ley declaran exentas de la autoridad pública. Dichas pruebas serán admitidas cuando el proceso fuera promovido por la publicación de censuras a la conducta pública de los funcionarios del Estado, y en los demás casos establecidos expresamente por la ley".

Articulo 28. Del derecho a Informarse (párrafo final): "(…) Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios"

Convención de Ciberdelincuencia de Budapest en el sistema penal paraguayo. La Convención sobre Ciberdelincuencia creada en el año 2001. El 20 de diciembre del 2017, a través de la Ley 5994/17 el Paraguay se adhirió oficialmente al Convenio sobre Ciberdelito del Consejo de Europa, adoptado en la ciudad de Budapest el 23 de noviembre de 2001. El Paraguay, al adherirse al Convenio de Budapest puede beneficiarse de estar en la lista de países respaldados por el Proyecto GLACY+.

La ratificación del Convenio fue positiva para el Paraguay ya que la legislación resultaba aún insuficiente para considerar satisfactoria la política criminal en el ámbito de persecución de este tipo de hechos, al no contar con uno de los elementos más importantes para la investigación de los delitos informáticos, que radica en la cooperación internacional.

La armonización de este instrumento internacional al sistema penal interno, era imprescindible para acceder a las evidencias electrónicas, incautación de pruebas a través de sistemas informáticos, retención de datos de tráfico entre otros porque muchas de estas acciones procesales conllevan la violación de la Constitución Nacional paraguayo y los derechos humanos.

Esta convención internacional aborda las conductas delictivas que se cometen a través de Internet y a su vez la persecución penal transfronteriza de los mismos y así reducir la incidencia de “refugios seguros” para el cibercrimen.

El citado instrumento internacional tiene el objetivo de armonizar las legislaciones de los estados miembros de la Unión Europea en un primer momento, pero abierto a la aprobación de los demás países a partir del mes de noviembre del mismo año. De este modo, que Paraguay sumó mas de 50 países que la han aprobado.

Ley Nº 4439/11. La presente ley se incorporó al orden jurídico penal varias figuras que tipifican adecuadamente los delitos informáticos, tales como: el acceso indebido a datos -o hacking-, el sabotaje a sistemas informáticos, la interceptación de datos o el acceso indebido a sistemas informáticos, los que fueron agregados a los tipos penales establecidos originariamente en el Código Penal

El art. 1° de la Ley Nº 4439/2011, que amplía el art. 146 del Código Penal Paraguayo (Ley Nº 1167/97), y por el cual queda como sigue: art. 146b – Acceso indebido a datos, que reza:

1°. El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa.

Al iniciar el análisis se desprende que la norma prohíbe obtener datos protegidos contra acceso no autorizado, sin consentimiento y violando los sistemas de seguridad.

Al ser un tipo penal novedoso, que ha surgido de la evolución de la informática y su influencia en la sociedad actual, determinar el bien jurídico protegido es aún confuso.

Como delito de mera actividad, en la que el resultado del acto es irrelevante para su penalización, se debe individualizar cual es el ámbito de protección de la norma. Aquí nos encontramos con que el Derecho a la Intimidad, tanto de personas físicas como personas jurídicas, se desprende como un derecho inalienable a proteger.

Ley Nº. 2861/2006, que Reprime el Comercio y la Difusión Comercial o no Comercial de Material Pornográfico, Utilizando la Imagen u otra Representación de Menores o Incapaces.

Artículo 1. Utilización de niños, niñas y adolescentes en pornografía

El que, por cualquier medio produjese o reprodujese un material conteniendo la imagen de una persona menor de dieciocho años de edad en acciones eróticas o actos sexuales que busquen excitar el apetito sexual, así como la exhibición de sus partes genitales con fines pornográficos, será castigado con pena privativa de libertad de cinco a diez años.

Artículo 2. Difusión o Comercialización de pornografía infantil.

El que distribuyese, importase, exportase, ofertase, canjease, exhibiese, difundiese, promocionase o financiase la producción o reproducción de la imagen de que trata el Artículo 1°, será castigado con pena privativa de libertad de tres a ocho años.

Artículo 3. Exhibición de niños, niñas y adolescentes en actos sexuales.

El que participase en la organización, financiación o promoción de espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años de edad en acciones eróticas de contenido sexual, será castigado con pena privativa de libertad de cinco a diez años.

Artículo 4. Agravantes. La pena privativa de libertad establecida en los artículos anteriores, será aumentada hasta quince años, cuando:

1.- La víctima fuere menor de quince años de edad; o,

2.- El autor:

1. tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;

2. operará en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente; o,

3. hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie.

Artículo 5. Pena Complementaria y Comiso Especial.

Cuando el autor actuara comercialmente o como miembro de una banda que se ha formado para la realización de hechos señalados en los artículos anteriores, se aplicará lo dispuesto en los Artículos del Código Penal referentes a la pena patrimonial y el comiso especial extensivo.

Artículo 6. Consumo y posesión de pornografía infantil.

1.- El que adquiriese o, a cualquier otro título, poseyese la imagen con las características descriptas en el Artículo 1° de la presente Ley, será castigado con pena privativa de libertad de seis meses a tres años.

2.- Con la misma pena será castigado el que asistiese al espectáculo descripto en el Artículo 3 de la presente Ley, salvo cuando por las circunstancias del caso no haya podido prever la realización de lo descripto en dicho artículo y que, habiéndose percatado de ello, inmediatamente se hubiese retirado del lugar y denunciado el hecho.

Artículo 7. Obligación especial de denunciar. Persecución y ejecución penal.

Toda persona que presencie la realización de los hechos punibles descriptos en los Artículos 1°, 2° y 3° de la presente Ley, está obligada a:

1. Denunciar sin demora a la Policía o al Ministerio Público;

2. Aportar, en caso que posea, los datos para la ubicación, incautación y eventualmente, la destrucción de la imagen, así como para la individualización, aprehensión y sanción del o los autores.

El que incumpliese estas obligaciones será castigado con pena privativa de libertad de hasta tres años o con multa, salvo que razonablemente arriesgue su propia persecución penal. Quienes detenten la patria potestad, o soporten un deber legal de guarda o tutela respecto del niño o adolescente directamente afectado por el hecho, no podrán invocar la

exoneración prevista en el Código Procesal Penal para quienes arriesguen la propia persecución penal o de un pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, ni la eximición de pena prevista en el Código Penal.

Artículo 8. Prohibición de Medidas Sustitutivas y Alternativas a la Prisión Preventiva y de Libertad Condicional.

Los procesados por la comisión de hechos punibles descriptos en esta Ley, no podrán ser beneficiados con medidas sustitutivas o alternativas a la prisión preventiva. Los condenados por la comisión de hechos punibles descriptos en esta Ley, no podrán ser beneficiados con el régimen de libertad condicional.

Artículo 9. Protección de Derechos y Garantías durante la persecución penal.

En la investigación y persecución de los hechos contemplados en los Artículos 1º, 2º, 3º y 6º de la presente Ley, se observarán las siguientes disposiciones de protección de los derechos y garantías del imputado y del interés superior del niño, niña y adolescente:

1.- Las imágenes que estén en poder del Ministerio Público, no serán entregadas a las partes ni exhibidas a terceros.

2.- Se labrará un Acta del contenido de las imágenes, el cual quedará a disposición de las partes y tendrá siempre carácter reservado.

3.- El imputado podrá estar presente en el momento de labrarse el Acta. Si no hubiese comparecido al acto por sí o por intermedio de su defensor, podrá solicitar al Juez de Garantías, que las imágenes le sean exhibidas en audiencia reservada a las partes. Sus observaciones se harán constar en Actas.

4.- Las imágenes no serán reproducidas, salvo cuando el Juzgado disponga lo contrario, mediante resolución que sólo podrá fundarse en la conservación del medio de prueba. La parte que solicitó la medida podrá recurrir la resolución que la rechace. El Ministerio Público y la víctima podrán recurrir la resolución que la otorgue.

5.- Las personas que accediesen a las imágenes, en razón a su función pública o actividad profesional, de acuerdo a las disposiciones de este artículo o de otras leyes, son

personalmente responsables de evitar que su contenido sea total o parcialmente reproducido, difundido o divulgado.

Artículo 10. Violación de derechos con motivo del proceso. El que incumpliese las disposiciones del artículo anterior, será castigado con pena privativa de libertad de cinco a diez años.

Ley 4468/13 de Comercio Electrónico. Es una normativa que en el artículo 10 – Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas de la Ley Nº 4468 (Congreso Nacional, 2013) , obliga a las empresas proveedoras de Internet en Paraguay (ISPs) y proveedores de servicios de alojamiento de datos a almacenar como mínimo 6 meses los datos de tráfico o "relativos a la comunicaciones electrónicas". (Sequera & Samaniego, 2018)

Algunas ISPs en Paraguay limitan el acceso al poder judicial y policial, porque su interpretación se basa en que la misma es exclusivamente para fines comerciales. Sin embargo, la ISP estatal COPACO facilita los datos de tráfico para las persecuciones penales solicitadas a través de pedidos de Informes del Ministerio Público. (Sequera & Samaniego, 2018)

Esta medida es preocupante porque se interpretan los datos de tráfico como información "insignificante" en el conjunto de la comunicación del usuario, por lo que no se considera parte de la comunicación. Como se expuso en la sección anterior "sobre los datos de tráfico o metadatos", esto es erróneo, ya que existe jurisprudencia internacional que ha demostrado que los metadatos forman parte de la comunicación y su inviolabilidad, obligando a las autoridades penales a otorgar acceso a los mismos solo de forma excepcional y a través de una orden judicial debidamente justificada. (Sequera & Samaniego, 2018)

Ley Nº 1328/98: De Derecho de Autor y Derechos Conexos.

Artículo 120. La protección reconocida a los derechos conexos al derecho de autor, y a otros derechos intelectuales contemplados en el presente Título, no afectará en modo alguno la tutela del derecho de autor sobre las obras literarias o artísticas. En consecuencia, ninguna de las disposiciones contenidas en el presente Título podrá interpretarse en

menoscabo de esa protección. En caso de duda o conflicto se estará a lo que más favorezca al autor.

Sin perjuicio de sus limitaciones específicas, todas las excepciones y límites establecidos en esta ley para el derecho de autor, serán también aplicables a los derechos reconocidos en el presente Título.

Artículo 121. Los titulares de los derechos conexos y otros derechos intelectuales podrán invocar las disposiciones relativas a los autores y sus obras, en cuanto estén conformes con la naturaleza de sus respectivos derechos.

Artículo 134. La presente ley reconoce un derecho de explotación sobre las grabaciones de imágenes en movimiento, con o sin sonido, que no sean creaciones susceptibles de ser calificadas como obras audiovisuales. En estos casos, el productor gozará, respecto de sus grabaciones audiovisuales, del derecho exclusivo de autorizar o no su reproducción, distribución y comunicación pública, inclusive de las fotografías realizadas en el proceso de producción de las grabaciones audiovisuales.

La duración de los derechos reconocidos en este artículo será de cincuenta años, contados a partir del uno de enero del año siguiente al de la divulgación de la grabación o al de su realización, si no se hubiere divulgado.

Artículo 135. Quien realice una fotografía u otra fijación obtenida por un procedimiento análogo, que no tenga el carácter de obra de acuerdo a la definición contenida en el numeral 16 del Artículo 21 y de lo dispuesto en el Título II de esta ley, goza del derecho exclusivo de autorizar su reproducción, distribución y comunicación pública, en los mismos términos reconocidos a los autores fotográficos.

La duración de este derecho será de cincuenta años contados a partir del uno de enero del año siguiente a la realización de la fotografía.

Artículo 148. La Dirección Nacional del Derecho de Autor podrá imponer sanciones a las entidades de gestión que infrinjan sus propios estatutos o reglamentos, o que incurran en hechos que afecten los intereses de sus representados, sin perjuicio de las sanciones penales o las acciones civiles que correspondan.

Artículo 149. Las sanciones a que se refiere el artículo anterior podrán ser:

1. amonestación privada y escrita;

2. amonestación pública difundida a través de los medios de comunicación social que designe la Dirección, a costa de la infractora;

3. multa que no será menor de diez salarios mínimos ni mayor de cien salarios mínimos, de acuerdo a la gravedad de la falta;

4. suspensión de la autorización para su funcionamiento hasta por un año; y,

5. cancelación del permiso de funcionamiento en casos de particular gravedad.

Artículo 150. Las infracciones a esta ley o a sus reglamentos, serán sancionadas por la Dirección Nacional del Derecho de Autor, previa audiencia del infractor, con multa por el equivalente de diez a cien salarios mínimos. En caso de reincidencia, que se considerará como tal la repetición de un acto de la misma naturaleza en un lapso de seis meses, se podrá imponer el doble de la multa.

Artículo 151. Contra las resoluciones emitidas por la Dirección Nacional del Derecho de Autor, se podrá apelar ante el Ministro de Industria y Comercio. El recurso será interpuesto ante el Director de la misma dentro de cinco días hábiles. El Ministro dictará resolución fundada y contra ella podrá interponerse recurso contencioso- administrativo dentro de diez días hábiles.

Transcurridos quince días hábiles sin que el Ministro dicte Resolución, el interesado podrá recurrir directamente a la vía contencioso-administrativa.

Artículo 166. Se impondrá una pena de seis meses a un año de prisión o multa de cinco a cincuenta salarios mínimos, a quien estando autorizado para publicar una obra, dolosamente lo hiciere en una de las formas siguientes:

1. sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador;

2. estampe el nombre con adiciones o supresiones que afecten la reputación del autor como tal o, en su caso, del traductor, adaptador, compilador o arreglador;

3. publique la obra con abreviaturas, adiciones, supresiones o cualesquiera otras modificaciones, sin el consentimiento del titular del derecho;

4. publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto cuando solamente se le haya autorizado la publicación de ellas en forma separada.

Artículo 167. Se impondrá pena de prisión de seis meses a tres años o multa de cien a doscientos salarios mínimos, en los casos siguientes:

1. al que emplee indebidamente el título de una obra, con infracción del Artículo 61 de esta ley;

2. al que realice una modificación de la obra, en violación de lo dispuesto en el Artículo 30 de la presente ley;

3. al que comunique públicamente una obra, en violación de lo dispuesto en el Artículo 27; una grabación audiovisual, conforme al Artículo 134; o una imagen fotográfica, de acuerdo al Artículo 135 de esta ley;

4. al que distribuya ejemplares de la obra, con infracción del derecho establecido en el Artículo 28; de fonogramas, en violación del Artículo 127; de una grabación audiovisual conforme al Artículo 134; o de una imagen fotográfica de acuerdo al Artículo 135 de la presente ley;

5. al que importe ejemplares de la obra no destinados al territorio nacional, en violación de lo dispuesto en el Artículo 29; o de fonogramas, infringiendo lo dispuesto en el Artículo 127 de esta ley;

6. al que retransmita, por cualquier medio alámbrico o inalámbrico, una emisión de radiodifusión o una transmisión por hilo, cable, fibra óptica u otro procedimiento análogo, infringiendo las disposiciones de los Artículos 25, 26, 131 ó 132 de esta ley;

7. al que comunique públicamente interpretaciones o ejecuciones artísticas, o fonogramas, que estén destinados exclusivamente a su ejecución privada;

8. al que, siendo cesionario o licenciatario autorizado por el titular del respectivo derecho, reproduzca o distribuya un mayor número de ejemplares que el permitido por el contrato; o comunique, reproduzca o distribuya la obra, interpretación, producción o emisión, después de vencido el plazo de autorización que se haya convenido;

9. a quien dé a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular; y,

10. a quien fabrique, importe, venda, arriende o ponga de cualquier otra manera en circulación, dispositivos o productos o preste cualquier servicio cuyo propósito o efecto sea impedir, burlar, eliminar, desactivar o eludir de cualquier forma, los dispositivos técnicos que los titulares hayan dispuesto para proteger sus respectivos derechos.

Artículo 168. Se impondrá pena de prisión de dos a tres años o multa de doscientos a mil salarios mínimos, en los casos siguientes:

1. al que se atribuya falsamente la cualidad de titular, originario o derivado, de cualquiera de los derechos reconocidos en esta ley, y con esa indebida atribución obtenga que la autoridad competente suspenda el acto de comunicación, reproducción, distribución o importación de la obra, interpretación, producción, emisión o de cualquiera otro de los bienes intelectuales protegidos por la presente ley;

2. al que presente declaraciones falsas en cuanto a certificaciones de ingresos, repertorio utilizado, identificación de los autores, autorización supuestamente obtenida, número de ejemplares o toda otra adulteración de datos susceptible de causar perjuicio a cualquiera de los titulares de derechos protegidos por esta ley;

3. a quien reproduzca, con infracción de lo dispuesto en el Artículo 26, en forma original o elaborada, íntegra o parcial, obras protegidas, salvo en los casos de reproducción lícita taxativamente indicados en el Capítulo I del Título V; o por lo que se refiera a los

programas de ordenador, salvo en los casos de excepción mencionados en los Artículos 70 y 71 de esta ley;

4. al que introduzca en el país, almacene, distribuya mediante venta, renta o préstamo o ponga de cualquier otra manera en circulación, reproducciones ilícitas de las obras protegidas;

5. a quien reproduzca o copie, por cualquier medio, la actuación de un artista intérprete o ejecutante; o un fonograma; o una emisión de radiodifusión o transmisión por hilo, cable, fibra óptica u otro procedimiento análogo; o que introduzca en el país, almacene, distribuya, exporte, venda, alquile o ponga de cualquier otra manera en circulación dichas reproducciones ilícitas; 6. al que inscriba en el Registro del Derecho de Autor y Derechos Conexos, una obra, interpretación, producción, emisión ajenas o cualquiera otro de los bienes intelectuales protegidos por esta ley, como si fueran propios, o como de persona distinta del verdadero titular de los derechos; y, 7. a quien fabrique, importe, venda, arriende o ponga de cualquier otra manera en circulación, dispositivos o sistemas que sean de ayuda primordial para descifrar sin autorización una señal de satélite codificada portadora de programas o para fomentar la recepción no autorizada de un programa codificado, radiodifundido o comunicado en otra forma al público.

Artículo 170. Se impondrá pena de prisión de dos a tres años o multa de cien a doscientos salarios mínimos a quien posea, use, diseñe, fabrique, importe, exporte o distribuya ya sea por venta, arrendamiento, préstamo u otro, cualquier artefacto, programa de computación o contra quien haga la oferta de realizar o realice un servicio, cuyo objetivo sea el de permitir o facilitar la evasión de tecnología de codificación.

Resoluciones Nº 3459/10 y 4408/11. El Ministerio Publico, por Resolución de la Fiscalía General del Estado, F.G.E. Nº 3459/2010 creó la Unidad Especializada de Delitos Informáticos y amplía sus funciones por Resolución F.G.E. Nº 4408/2011, para hacer frente a aquellos hechos punibles que derivan del uso mal intencionado de la tecnología. La iniciativa surge como respuesta a la necesidad de combatir de manera frontal y eficiente estos delitos. La Unidad tiene jurisdicción en todo el territorio nacional, es la principal autoridad a cargo de la investigación y de la acción judicial en casos de delitos informáticos, tales como alteración

de datos en computadora, sabotaje de computadoras, operaciones fraudulentas por computadoras, alteración de datos relevantes para la prueba, entre otros.

Es importante resaltar que el Ministerio Público es la única autoridad gubernamental capaz de solicitar información a los prestadores de servicio internacionales cuando dicha información sea necesaria para una investigación. Por otro lado, el Código Procesal Penal, Ley Nº 1286/98, establece que cualquier persona conocimiento referente a un acto punible por parte del Estado deberá compartir dicha información con el Ministerio Público o con la Policía Nacional. (Valiente & Giovanni , 2016)

Sanciones a los delitos informáticos

Violación del secreto de la comunicación: Artículo 146 del Código Penal.

1º El que, sin consentimiento del titular:

1. abriera una carta cerrada no destinada a su conocimiento;

2. abriera una publicación (escrito, cinta portadora de sonido e imágenes, reproducciones y demás medio de registros), en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación;

3. lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero, será castigado con pena privativa de libertad de hasta un año o con multa.

2º La persecución penal dependerá de la instancia de la víctima. Se aplicará lo dispuesto en el artículo 144, inciso 5º, última parte.

Este bien jurídico parte del derecho que tiene toda persona a la intimidad, no referida a un espacio físico, sino a un determinado ambiente inmaterial de la intimidad, reconocida por la ley como personal, propio e inviolable; desde este punto de vista, se reconoce una esfera de la intimidad, dentro de la cual las cosas son secretas en la medida en que son consideradas una prolongación de la persona misma. De ahí que no sea necesaria ninguna investigación para establecer, en el, caso concreto, si la carta, pliego, telegrama o cualquier documento de naturaleza análoga contiene o no un secreto; la lesión del bien jurídico se

produce ya por el simple hecho de existir una intromisión en una esfera personal, dentro de la cual los objetos son íntimos. (Arias, 2013)

El derecho a la intimidad es un bien jurídico protegido constitucionalmente por el Paraguay, la comunicación forma parte de la intimidad del ser humano, es así, que ninguna persona está autorizada a inspeccionarla sin autorización de la autoridad competente. La omisión de las normativas establecidas en relación a este derecho serán penadas conforme al código penal que prevé una sanción de 1 año o multa.

Alteración de datos (interferencia): Artículo 174 del Código Penal.

1º El que lesionando el derecho de disposición de otro sobre datos los borrará, suprimiera, inutilizará o cambiará, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º En estos casos, será castigada también la tentativa.

3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

Como ya se ha mencionado en otro apartado, la alteración de datos consiste en cierta modificación en los datos originarios, ese flagelo se encuentra tipificado en el código penal a lo cual se le otorga una sanción de pena privativa de libertad de dos años o multa según corresponda.

Sabotaje de computadoras: Artículo 175 del Código Penal.

1º 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; o

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.

2º En estos casos, será castigada también la tentativa.

Sánchez (2018) define al sabotaje “El sabotaje, se define como aquel acto delictual, y deliberado, en que se daña o destruye, bienes públicos o privados, con el objeto de anular su funcionamiento, o derechamente ponerlos fuera de servicio”

El sabotaje busca adulterar datos o destruir medios para evitar su procesamiento, será sancionado conforme lo establece el código penal, con cinco años de cárcel o muta.

Falsificación Informática. Alteración de datos relevantes para la prueba: Artículo 248 del Código Penal.

1º El que, con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, será castigada también la tentativa.

3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º

La Falsificación Informática es el término genérico que se usa para aquellas operaciones ilícitas realizadas por medio de la Internet. La existencia de puntos de contacto entre la falsificación de documentos electrónicos y el sabotaje informático resultan indesmentibles.

La sanción que establece el código penal paraguayo para dicho acto antijuridico es de cinco años o con multa.

Fraude Informático: Artículo 188 del Código Penal.

1º 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; o

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.

2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos

2º al 4º. Ley 3440/07 - Pornografía relativa a niños y adolescentes. “Art. 140: El que por cualquier medio produjere publicaciones que contengan como temática actos sexuales…” Art. 143: Lesión a la intimidad de las personas.: El que mediante publicación expusiera la intimidad de otro…..

El fraude informático es el acto de usar una computadora para tomar o alterar datos electrónicos, o para obtener un uso ilegal de una computadora o sistema, bajo esta denominación, el código penal paraguayo sanciona este hecho ilícito con pena privativa de libertad de hasta cinco años o con multa.

Pornografía Infantil: Artículo 140 de la Ley 3440/07.

1º.- El que:

1. por cualquier medio produjere publicaciones, que contengan como temática actos sexuales con participación de personas menores de dieciocho años de edad y que busquen excitar el apetito sexual, así como la exhibición de sus partes genitales con fines pornográficos;

2. organizará, financiara o promocionará espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales; o

3. distribuyera, importara, exportara, ofertara, canjeará, exhibiera, difundiera, promocionará o financiará la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa.

2º.- El que reprodujera publicaciones según el numeral 1 del inciso 1º, será castigado con pena privativa de libertad de hasta tres años o multa.

3°.- La pena de los incisos anteriores podrá ser aumentada hasta diez años, cuando:

1. las publicaciones y espectáculos en el sentido de los incisos 1º y 2º se refieran a menores de catorce años;

2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;

3. el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente;

4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o

5. el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados.

4°.- El que con la intención prevista en el numeral 1 del inciso 1º obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3º, será castigado con pena privativa de libertad de hasta tres años o con multa.

5°.- Se aplicará, en lo pertinente, también lo dispuesto en los artículos 57 y 94.

6°.- Los condenados por la comisión de hechos punibles descriptos en este artículo, generalmente no podrán ser beneficiados con el régimen de libertad condicional.”

Marco Conceptual

Hechos Punibles: El código penal en su Artículo 14 expone: “Hecho Punible, es un hecho antijurídico que sea reprochable y reúna, en su caso, los demás presupuestos de la punibilidad”

Delitos informáticos: son todas las acciones dirigidas a lesionar la integridad, disposición y confiabilidad de datos y de sistemas informáticos, así como aquellas conductas que atentan contra el patrimonio de las personas utilizando herramientas tecnológicas e informáticas. (Unidad Especializada de Delitos Informáticos, 2018)

Regulación: Regulación es la acción y efecto de regular (ajustar o poner en orden algo, reglar el funcionamiento de un sistema, determinar normas). El término suele utilizarse como sinónimo de normativa. La regulación, por lo tanto, consiste en el establecimiento de normas, reglas o leyes dentro de un determinado ámbito. (Definicion.DE, 2021)

Legislación: Conjunto o cuerpo de leyes por las cuales se gobierna un Estado o se regula una materia determinada. (Ossorio, 2008)

Sanción: la palabra sanción se aplica al castigo que alguien recibe por haber violado una norma moral, social, religiosa o jurídica. (Deconceptos.com, s.f.)

Matriz de Operacionalización de Variables

Variable	Dimensión	Indicadores	Técnica e Instrumento
Paraguay en el afrontamiento de los delitos informáticos	Hechos punibles informáticos tipificados en la legislación paraguaya	- Preparación al acceso indebido a datos - Alteración de datos Acceso indebido a sistemas informáticos - Sabotaje a sistemas informáticos - Alteración de datos relevantes - Falsificación de tarjetas de crédito y débito - Estafa mediante sistemas informáticos	Revisión bibliográfica
	Normativas que protegen al individuo de los delitos informáticos	- Constitución Nacional Convención de Budapest - Ley Nº 4439/11 - Ley Nº. 2861/2006 - Ley 1328 del Derecho del Autor y Derechos conexos -Ley 4468/13 de Comercio Electrónico	

		Resoluciones Nº 3459/10 y 4408/11	
	Sanción prevista para los delitos informáticos	- Interceptación ilícita: Artículo 146 del Código Penal Interferencia en los Datos: - Artículo 174 del Código Penal - Interferencia en el Sistema: Artículo 175 del Código Penal - Falsificación Informática: Artículo 248 del Código Penal - Fraude Informático: Artículo 188 del Código Penal	

Marco Metodológico

Tipo de Investigación

Según su naturaleza, fue de un enfoque cualitativo, ya que se orienta a profundizar casos específicos y no a generalizar, al respecto Bernal, (2010) indica. “Su preocupación no es prioritariamente medir, sino cualificar y describir el fenómeno social a partir de rasgos

determinantes, según sean percibidos por los elementos mismos que están dentro de la situación estudiada"

Con respecto a esta investigación en forma específica se centró en lo concerniente a los hechos punibles informáticos y su regulación en la legislación paraguaya. Teniendo como base la normativa, la doctrina y la jurisprudencia

Nivel de Investigación según alcance

La investigación tendrá un alcance descriptivo porque describe los fenómenos, situaciones, contextos y sucesos; esto es, detallar cómo son y se manifiestan. Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2014)

La investigación, se encarga de puntualizar las características de la punibilidad de las acciones que conllevan a la realización de un hecho antijuridico que corresponde al delito informático. Esta metodología se centra más en el "qué", en lugar del "por qué" del objeto de la investigación.

Método de la Investigación

El método a implementar es el inductivo porque utiliza el razonamiento para obtener conclusiones que parten de hechos particulares aceptados como válidos, para llegar a conclusiones cuya aplicación sea de carácter general. El método se inicia con un estudio individual de los hechos se formulan conclusiones universales que se postulan como leyes, principios o fundamentos de una teoría. (Bernal, 2010)

Técnicas e Instrumentos de Recolección de Datos

Para la recolección de datos se manipuló la revisión de la Literatura, ya que nos enfocamos en la búsqueda de las diferentes fuentes documentales que proporcionan una base teórica a los delitos informáticos, una vez obtenida las mismas, se analiza los diferentes materiales para el cumplimiento de los objetivos propuestos.

Plan de Procesamiento de datos

La información recolectada fue procesada de manera selectiva, la misma es extraída, recopilada y clasificada según el orden de preponderancia. Primeramente, se procedió a

consultar a investigaciones anteriores para poder obtener un panorama preliminar de las doctrinas adoptadas en diversos países a los hechos punibles ejecutados transgrediendo la seguridad informática, posteriormente se clasifico las doctrinas más relevantes con posturas análogas conformando una legislación comparada y se inicia a recopilar los materiales poco extensos que se poseen en el Paraguay.

Análisis de datos obtenidos

Una vez conformada el cuerpo de la investigación, se procede a categorizar las manifestaciones resaltantes en cada material consultado, de esta manera reunimos y sintetizamos los datos relevantes dentro de la investigación para determinar objetivamente la intervención de la legislación paraguaya en relación a la comisión de los delitos informáticos.

Marco Analítico

Conclusiones

La investigación realizada, ha dejado como resultados las siguientes afirmaciones:

Los hechos punibles que se desprenden del uso del internet son variados, en todos los países del mundo, se detectan delitos contra la integridad física, sexual, contra los bienes materiales, la economía personal y del Estado que a diario emergen a raíz del uso de la tecnología. Paraguay en su caso, reconoce como delitos informáticos al acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas informáticos, sabotaje a sistemas informáticos, alteración de datos

relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos.

Las normativas que establece la Republica del Paraguay para proteger al individuo de los delitos informáticos se central en el Convención de Budapest, la Ley Nº 4439/11, las Resoluciones Nº 3459/10 y 4408/11, la Ley Nº. 2861/2006, La ley del comercio electrónico, Ley 1328 del Derecho del Autor y Derechos conexos.

El Convención de Budapest es una normativa de carácter internacional ratificada por el Paraguay para unificar las normativas en relación a los delitos informáticos cuando dos o más países se vean involucrados en un mismo hecho punible sobre el delito informático, por su parte, la Ley Nº 4439/11 ha incorporado algunas modificaciones dentro del Código penal para adaptarlo a las necesidades actuales en relación a los delitos perpetrados por medio del sistema informático. Las Resoluciones Nº 3459/10 y 4408/11 otorgan la competencia suficiente para intervenir a la Unidad Especializada en Delitos Informáticos en los tipos penales ya mencionados en el primer párrafo de la presente.

Los delitos informáticos son hechos punibles que surgieron a raíz de la era tecnológica, por tal motivo, el código penal paraguayo debió de ser modificado para que este se ajuste a la realidad delictiva de esta nueva era. Es así, que las penalidades se encuentran estipuladas en el código penal paraguayo, estableciendo sanciones de 1 año o multa, en algunos casos 5 años, y otros como la pornografía infantil, hasta 10 años.

La pregunta general se centra en la prerrogativa ¿Cómo afronta Paraguay los delitos informáticos?, analizando todos los datos recabados para describir la manera que afronta Paraguay los delitos informáticos, se llega a comprender que la Constitución Nacional, no se pronuncia específicamente sobre la virtualidad de los delitos, pero, cuenta con fuerte protección constitucional a la intimidad y la inviolabilidad de la comunicación de las personas, así como el derecho a la autodeterminación informativa.

Técnicamente, Paraguay posee una escasa normativa en relación a este tipo de flagelo, como ya se ha indicado, Paraguay hace alusión a varias normativas que luchan contra los delitos informático, pero no están enunciados implícitamente como tal, como lo es el caso de los derechos del autor. Paraguay se centra en pocas figuras delictivas, ignorando muchas otras que pudieran surgir de la virtualidad, es esta circunstancia, uno de los elementos con el que Paraguay cuenta para luchar contra este tipo de delitos es el convenio de Budapest para

prevenir las conductas que atenten contra la confidencialidad, integridad, disponibilidad de los datos y de los sistemas informáticos, pero lo más importante radica en su finalidad de establecer un marco jurídico internacional que permita impulsar la cooperación internacional.

Bibliografía

Alcívar Trejo, C., Domenech Alvarez, G., & Ortìz Chimbo, K. (2015). *La seguridad juridica frente a los delitos informaticos.* Ecuador.

Bernal, C. A. (2010). *Metodologia de la Investigacion.* Colombia.

Centurión, A. A. (2010). *Legislacion Paraguaya para el Delito Informatico.* Asuncion.

Ceresole, A., & Oyarzábal, S. (2014). *Delitos Informaticos.* Buenos Aires.

Deconceptos.com. (s.f.). Obtenido de https://deconceptos.com/ciencias-juridicas/sancion

Definicion.DE. (2021). *Regulacion*. Obtenido de https://definicion.de/regulacion/

Diccionario Panhispánico del español juridico. (2020). *alteración de datos y sabotaje informático*. Obtenido de https://dpej.rae.es/lema/alteraci%C3%B3n-de-datos-y-sabotaje-inform%C3%A1tico

Direccion contra Hechos Punibles econimicos y financieros de la Policia Nacional. (2016). *Policia Nacional*. Obtenido de Procedimiento contra acceso indebido a datos: http://www.delitoseconomicos.gov.py/index.php/noticias/procedimiento-contra-acceso-indebido-a-datos

Girala, F. (2020). *El mundo, la tecnología y los Delitos Informáticos en el Paraguay.* Asuncion.

Gomez, A. D. (2010). *El Delito Informatico, su problematica y su cooperacion internacional como paradigma de su solucion: El convenio de Budapest.* Peru.

Gonzalez, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). *Delitos Informaticos: Una revision en Latinoamerica.* Ecuador.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodologia de la Investigacion Cientifica.* Mexico: sexta.

Lux, L. M. (2017). *El bien juridico protegido en los delitos informaticos.* Chile.

Lux, L. M. (2018). *Elementos criminológicos para el análisis jurídico/penal.* Chile.

Ministerio Publico. Republica del Paraguay. (2018). Obtenido de Delitos Informaticos: https://ministeriopublico.gov.py/unidad-especializada-de-delitos-informaticos-

Montenegro, D. B. (2015). *El delito informático y su clasificación* .

Narváez Montenegro, B., & Recalde Machado, G. (2018). *El delito informativo en America.* Ecuador.

Ojeda Perez, J., Arias Flórez, M., Ricon Rodriguez, F., & Daza Martinez , L. (2010). *Delitos informáticos y entorno jurídico vigente en Colombia.* Colombia.

Ossorio, M. (2008). *Diccionario Juridico.* Asuncion.

Pino, S. A. (2016). *Delitos Informáticos: Generalidades.* Ecuador.

Preda, R. (23 de Enero de 2012). Ley contra los delitos informaticos. Breve Reseña. *abc color*.

Proteccion Online.com. (2012). Recuperado el 17 de Mayo de 2021, de https://www.protecciononline.com/leyes-que-regulan-los-delitos-informaticos-en-paraguay/

Sequera, M., & Samaniego, M. (2018). *Desafios de la Armonizacion de la convencion de budapest en el sitema penal paraguayo.* Asuncion. Obtenido de https://www.tedic.org/wp-content/uploads/2018/10/minuta_TEDIC.pdf

Unidad Especializada de Delitos Informáticos. (2018). *Ministerio Publico* . Obtenido de https://www.ministeriopublico.gov.py/archivos/Archivos_pdf/Publicaciones/Materiales_Informativos/Unidad_Especializada_de_Delitos_Informaticos.pdf?time=1562085815711

Valdez, J. T. (2000). *Los Delitos informáticos.* Merida.

Valiente, G., & Giovanni , M. (2016). *Legister.com*. Obtenido de El hacker y sus conductas: https://py.lejister.com/pop.php?option=articulo&Hash=952a97e11b186e60b7b56e1fc23a658&print=1