Universidad Internacional de La Rioja (UNIR)

ESIT

Máster universitario en Seguridad Informática

Análisis de derecho comparado del perito informático

Trabajo Fin de Máster

Presentado por: Poma Alejandro, María Elizabeth

Director/a: Delgado Sotés, Juan José

Ciudad: Quito, Ecuador
Fecha:05-10-2019

Resumen

Este trabajo busca unificar en un solo compendio, la información que está dispersa, comparar las leyes y regulaciones de acceso público, como herramienta para el desarrollo de la actividad del perito judicial e informático, así como otras leyes de carácter general. Presenta un análisis comparativo de la legislación española vigente, como de otros países latinoamericanos y del mundo, basándose en el principio que toda norma tiene un ordenamiento jerárquico, siendo la cúspide la Constitución, tomando como referencia la pirámide de Kelsen. Lo que se busca concretamente con el desarrollo del presenta trabajo, es concientizar no solamente a los administradores de justicia, sino al público en general, que existen normativas vigentes en cada Estado, que sancionan el cometimiento de infracciones derivados del mal uso de las tecnologías, para lo cual es indispensable la labor que realizan los peritos informáticos, investigadores del campo científico que ayudan a sancionar a los delincuentes informáticos.

Palabras Clave: Ciberdelito, daño informático, delito informático, delito contra la propiedad intelectual perito informático, legislación comparada, legislación informática.

Abstract

This document seeks to unify in a single compendium, the information that is dispersed, to compare the laws and regulations of public access, as a tool for the development of the activity of the judicial and computer expert, as well as other laws of a general nature. It presents a comparative analysis of current Spanish legislation, as of other Latin American countries and the world, based on the principle that every rule has a hierarchical order, the Constitution being the cusp, taking as reference the Kelsen pyramid. What is specifically sought with the development of this work, is to raise awareness not only to the administrators of justice, but to the general public, that there are regulations in force in each State, which sanction the commission of infractions derived from the misuse of technologies, for which it is essential the work carried out by computer experts, researchers in the scientific field who help punish computer criminals.

Keywords: Cybercrime, computer damage, computer crime, intellectual property crime, computer expert, comparative legislation, computer legislation.

CONTENIDO

1 INTRODUCCIÓN

El constante avance tecnológico, admite el perfeccionamiento de delitos tradicionales, dando lugar a la aparición de nuevos ilícitos, denominados delitos informáticos. Estas nuevas formas de delinquir emplean hardware, software y redes interconectadas de comunicación, como es el caso de Internet. Este último, brinda una gran diversidad de recursos y servicios, que permiten al infractor pasar inadvertido. Las motivaciones para cometer estos ilícitos son diversas, que van desde económicas, culturales, espionaje, represalias, incluso por curiosidad y retos personales.

Las sociedades continuarán acelerando el uso de nuevas tecnologías y la dependencia de la conectividad a Internet, lo que nos plantea nuevos retos, por ejemplo, cómo reforzar la seguridad para impedir ser víctimas de estos ataques, y en caso de serlo, cómo actuar para que los culpables sean castigados.

Todo esto plantea interrogantes acerca de la existencia de fronteras para el cometimiento de estos delitos, lo que consecuentemente impone a las autoridades gubernamentales la obligación de contar con un marco normativo adecuado, así como de estrategias de investigación del delito eficaces, pues de ello dependerá que se logre una protección idónea frente a estas nuevas amenazas.

En este sentido, es menester que se logren acuerdos que promuevan y regulen el uso apropiado de la tecnología, porque la ausencia o vacíos de regulación punitiva hace que los delitos se vuelvan incontrolables para un solo Estado, debido a que el delito informático no tiene fronteras físicas, de allí que se requiere de herramientas que impidan que este tipo de conductas se cometan de manera trasnacional, y más aún, evadan las sanciones penales debido a la falta de acuerdo de cooperación binacional y multilateral de los Estados para sancionar a los infractores.

Precisamente, debe recordarse que la investigación del delito, implica un accionar multilateral, ya que por un lado se encuentran los profesionales del derecho, quienes ejercer las actividades jurídicas necesarias para la determinación de la existencia de un delito y de la responsabilidad de un infractor, pero los mismos están auxiliados por un conjunto de profesionales técnicos capacitados en diversas áreas del saber humano, que realizan las actividades de investigación del delito en los campos criminológicos, denominados como peritos.

En este sentido, uno de los integrantes más importantes en la lucha contra los delitos informáticos, son los peritos informáticos, quienes forman parte del sistema de administración

de justicia, y que se han de comprometido, además de ejercer sus actividades científicas, a conocer la legislación adoptada por ciertos Estados, así como los acuerdos transnacionales; a fin de no transgredir la protección de los derechos de las personas, y a la vez mantener su objetividad durante la investigación criminológica, para que la evidencia obtenida sirva de prueba incuestionable para poder determinar la existencia material del delito y el nexo causal con el presunto infractor.

2 OBJETIVOS

2.1 Objetivo general

- Realizar un compendio de información acerca de las leyes y regulaciones de los delitos informáticos, con énfasis en la normativa relacionada con la formación del perito informático.

2.2 Objetivos específicos

- Analizar desde la perspectiva doctrinaria la definición de los delitos informáticos y establecer cuáles son los tipos penales informativos más frecuentemente cometidos en el mundo.
- Conocer las disposiciones constitucionales y legales de los distintos países acerca de los delitos informáticos y las limitaciones que existen frente a cometer acciones punitivas.
- Establecer los aspectos positivos y las deficiencias normativas de cada una de las leyes que regulan la actividad del perito informático en la legislación de distintos países, principalmente la española y la ecuatoriana.
- Crear un compendio acerca de la información más importante que regula el nombramiento del perito informático, que sirva de base para la capacitación y guía de estos profesionales, sobre todo en aquellos países en donde no existe normativa especializada de esta materia.

3 CONTEXTO Y ESTADO DEL ARTE

En lo que se refiere al delito informático, su incorporación ha sido reciente dentro del ámbito del derecho penal, pues no ha sido sino hasta la expansión de las distintas tecnologías de la información, así como del uso en masa del internet, redes sociales, cuando ha empezado a existir una necesidad de protección frente a las diversas conductas que se cometían dentro del ciberespacio y que suponían una nueva forma de cometer delitos, mientras que en otros casos se crearon conductas típicas nuevas que podría presentarse solamente en este tipo de especio digital.

Es así que desde los años 80 y 90 se empezaron a llevar a cabo distintas investigaciones acerca de los dilemas que suponía el uso de internet y las repercusiones que existían dentro de campo jurídico, mismas que transigieron hacia el campo del derecho penal y extendieron a lo largo de los años subsiguientes, cuando se comprende la verdadera dimensión de como el internet y las tecnologías de la información podían ser utilizadas como un medio para el cometimiento del delito.

En este sentido, existieron obras pioneras en las cuales ya se abordan algunas de las conductas típicas del delito informático, entre las que se encuentra la realizada por el autor Alfredo Sneyers, denominada como “El fraude y otros delitos informáticos”, de 1990, en la cual se centra en las nuevas modalidades de fraude, así como también en la definición misma del delito informático.

Desde esta perspectiva, cabe puntualizar que el delito informático no constituye un tipo penal en concreto, sino más bien alude a una categoría de delitos que comparten un rasgo en común, que es la utilización del internet, otros medios electrónicos o tecnologías de la información para cometer un hecho ilícito.

Este hecho resulta particularmente novedoso, en el sentido de que la agrupación de lo estos delitos no se da en razón del bien jurídico que afectan, pues en este caso podrían ser varios los bienes afectados: patrimonio, integridad sexual, integridad física, salud, libertad, datos públicos, entre otros.

Asimismo en el año de 1998, el autor Jorge Pacheco Klein, publica su obra: “Introducción a los delitos informáticos en el ciberespacio: normas y jurisprudencia comentadas”, donde igualmente, se hace referencia al delito informático desde la perspectiva general, dando a conocer las particularidades de este tipo penal que recién se empezaba a dar a conocer a profundidad, pero también ya se destacan algunas de las normas en el mundo, que empiezan

a realizar un control exhaustivo de estas conductas y la jurisprudencia que va quedando sentada en los distintos tribunales en donde se conocen estas causas.

En el año 2000, el autor Pablo Andrés Palazzi publica su obra “Delitos informáticos”, en la cual estudia, asimismo, las particularidades y los elementos del delito informático, pretendiendo realizar un primer acercamiento conceptual de lo que implican estos nuevos delitos, que cuya estructura recién empezaba a tener una forma definida.

Posteriormente, un año más tarde, en el año 2001, el autor Carlos Tablante publica su obra bibliográfica “Delitos informáticos, delincuentes sin rostro: una propuesta legal para enfrentar las amenazas del ciberespacio”, en la cual ya comenzaba a plasmar algunos de los problemas más importantes que implicaban la persecución de este tipo de delitos, en razón de que la individualización del sujeto activo del delito, es decir, de quien comete la conducta tipificada dentro de la ley penal, resulta dificultosa, debido a que las facilidades que brindan el internet, les permite un mayor anonimato a los infractores, así como también debido al hecho de que las fronteras geográficas de los países no existen dentro del ciberespacio, por lo que fácilmente se puede cometer delincuencia trasnacional, haciendo más difícil la captura del infractor, al requerirse una cooperación multilateral de diversos países.

En este mismo año 2001, los autores Emilio del Peso Navarro y Carlos Manuel Fernández Sánchez publican una obra de gran importancia, denominada “Peritajes informáticos”, en el cual abordan la realidad del internet como una realidad que tiene cada día más importancia en todos los aspectos del ser humano, de allí la necesidad de conocer y regular estas situaciones jurídicas, pues es evidente que existe un aumento de la problemática jurídica que se da en torno a este fenómeno.

Los autores señalan que la necesidad de generar nuevos conocimientos acerca de esta realidad, es para beneficio del usuario, quien es la persona más vulnerable frente a las diferentes conductas delictivas que se pudieran producir a través de estos medios; pues si bien es cierto la tecnología ha sido un motor de impulso para las distintas sociedades humanas, la misma también tiene un lado desconocido y negativo, en donde los delincuentes la utilizan como una herramienta para delinquir y obtener impunidad de la justicia.

Precisamente en este contexto, los autores resaltan la importancia que tiene el perito informático, como una figura conocedora de los aspectos más importantes, pero a la vez desconocidos de la informática, que puede tener un papel importante a la hora de resolver un delito cometido por estas vías, de allí que deban destacarse la importancia de este profesional, facilitándose su labor a través de la existencia de un marco jurídico idóneo para que pueda cumplir con su labor.

Estudios mucho más elaborados acerca del delito informativo se pueden observar en los años cercanos al 2010, en donde se empiezan a estudiar por separado cada uno de los aspectos que componen el delito informático, pues mientras en algunas referencias bibliográficas se estudia el aspecto sustantivo de este delito, en otros se hace referencia a la parte procedimental del mismo.

Otro aspecto importante, es que se comienzan a estudiar cada uno de los delitos informáticos por separado, es decir, los delitos de terrorismo informático, pornografía infantil, vulneración de derechos de autor, ciberacoso, estafa por medios electrónicos, comienzan a desarrollarse en estudios bibliográficos de manera individual y con una perspectiva más amplia, utilizándose la parte sustantiva, pero también la adjetiva procedimental, lo que incluye lógicamente el estudio de la investigación del delito, donde toma gran protagonismo la labor pericial desarrollada en este campo.

Es así que, en el año 2009, la autora Ivonne Valeria Muñoz Torres, realiza la publicación de su obra bibliográfica “Delitos informáticos: diez años después”, que resulta importante en razón del contraste que presenta acerca del inicio de los delitos informáticos hasta el momento actual, en donde se nota una evolución del delito, pero además también se observa una evolución en la dogmática jurídica, que comprende de mejor manera la naturaleza jurídica de este tipo de delitos, lo que incluye lógicamente una labor mejorada de las instituciones de percusión del delito, fiscalía y unidades de investigación criminológica, en donde, a través de la labor de peritos en el campo informático se logra la sanción de los infractores.

Precisamente en este sentido, se destaca la obra del autor Luis Orlando Palomá Parra “Delitos informáticos (en el ciberspacio): doctrina y análisis de casos reales” del año 2012, en la cual, no solamente se analiza la doctrina más reciente acerca de los delitos informáticos, sino que la misma va acompañada de algunos casos reales en los cuales se puede ejemplificar la forma de actuación de los infractores en distintos de estos tipos penales.

A nivel internacional, en lo que se refiere a los organismos internacionales de investigación del delito, también se realizan importantes contribuciones, como en el caso del publicado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC por sus siglas en inglés), que se titula como “Estudio exhaustivo sobre el delito cibernético” del año 2013, que al igual que los demás manuales publicados por el UNODC, pretenden ser una pauta y referencia para todas las legislaciones nacionales acerca de cómo deben realizarse las investigaciones de los delitos informáticos, de allí que se combine tanto la información dogmática como la procedimental, incluyendo algunos aspectos del peritaje informático; pero además se dispone un capítulo dedicado al rol que tiene la ley, tanto nacional, como internacional, y la armonía que deberían guardar, para la persecución y sanción de este tipo de delitos.

En el año 2016, el autor Eloy Velasco Núñez publica su obra “Delitos tecnológicos: definición, investigación y prueba en el proceso penal: actualizado a las reformas del Código penal y de la Ley de enjuiciamiento criminal de 2015”, en la cual se contextualiza al delito informático en los últimos cinco años, pero además se aborda los aspectos procesales y probatorios que resultan de gran complejidad, todo ello en armonía con la evolución del marco normativo que debe ajustarse a las nuevas necesidades.

Así también, dentro de campo del peritaje informático existen notables avances en el aspecto bibliográfico, pues en el año 2016, los autores María Elena Darahuge, Luis E. Arellano González, publican su obra “Manual de informática forense”, que comprende tres tomos, en los cuales se abordan la prueba informática forense, la gestión integral de la prueba documental informática, y se realiza una guía de ejercicios para los peritos informáticos forenses.

Finalmente debe destacarse que, en el año 2018, los autores Ricardo Antonio Parada; José Daniel Errecaborde compilan varias obras relacionadas con esta temática, y la publican en la obra “Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet”, donde se recogen los aspectos más importantes de la investigación del delito informático.

Si bien es cierto, dentro de este conjunto de obras referidas, se hace un estudio acerca de la labor del perito informático, debe destacarse que en muy pocos, se realiza un contraste entre la normativa legal que regula su labor con la aplicación práctica, ni tampoco se compara las legislaciones para establecer los aciertos y las deficiencias, a fin de obtener una norma modelo que permita una mejor investigación de los peritos informáticos, labor que se pretende realizar en el presente documento.

4 DELITOS INFORMÁTICOS

4.1 Definición de delitos informáticos

Existen posturas que afirman que el delito informático no se trata de un nuevo concepto, sino que son las mismas acciones típicas, delitos y contravenciones tradicionales que afectan a distintos bienes jurídicos de la persona como el honor, la libertad, seguridad pública, los datos, la propiedad, la integridad sexual, entre otras; con la diferencia sustancial, que el origen de esta clase de criminalidad se encuentra ligado al desarrollo de nuevas tecnologías (En adelante TICs).

No existe un concepto único de lo que es un delito informático, los criterios no son uniformes de allí que es necesario analizar algunos de los mismos para comprender su alcance conceptual. En este sentido, la autora María de Luz Lima define al delito informático como:

> "En un sentido amplio es cualquier conducta criminógena o criminal que en su relación hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto el delito informático es cualquier acto ilícito penal, en las que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin" (Lima, 1984, pág. 321).

En la perspectiva de la autora se comprende como el delito informático constituye cualquier tipo de infracción penal que se haya acometido con la utilización de una TIC como un método, medio o fin, de allí que esta autora mantiene la línea de pensamiento de considerar que los delitos informáticos no son infracciones nuevas, sino las anteriormente previstas en la normativa penal, pero es su cometimiento el que varía de manera sustancial.

Por otro lado, respecto de la definición del delito informático, el autor Carlos Romeo Casabona manifiesta que:

> "En la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del -hecho delictivo o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información" (Romeo, 1988, pág. 9).

Desde la perspectiva planteada por el autor, se comprende como el delito informático constituye un término dinámico, en razón de que se adapta no solo a un tipo penal en concreto, sino que, al contrario, el mismo puede presentarse en diversas conductas delictivas que

afectan a diversos bienes jurídicos protegidos, y cuya característica en común, es el uso del computador como medio o instrumento para materializar esta infracción.

Por otra parte, existen definiciones mucho más complejas como la realizada por Donn Parker (1989) define a los delitos cibernéticos de acuerdo a los propósitos que se persiguen, de la siguiente manera:

> "Propósito de investigación de la seguridad: Se define como cualquier acto intencional o malicioso que involucre a un computador como objeto, sujeto, instrumento o símbolo donde una víctima sufrió o podría haber sufrido una pérdida y el perpetrador obtuvo o pudo haber obtenido una ganancia.
>
> Propósito de investigación y acusación: Delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática. (Departamento de Justicia de Estados Unidos).
>
> Propósito legal: Delito informático cualquier acto tipificado en una ley de acuerdo a la norma que se aplica en cada estado.
>
> Otros propósitos: Delito informático, cualquier delito cometido con ayuda de un computador" (Parker, 1989, pág. 11).

En la perspectiva del autor se comprende cómo la definición de delito informático se presenta de diversas formas, siendo la más común la que hace referencia al propósito, desde la cual, constituye cualquier acto en el que se haya utilizado al computador como un medio para el cometimiento del delito; mientras que, desde el punto de vista del sujeto, se comprende como delito informático, al realizado por una persona que tiene conocimientos acerca de esta disciplina de la ciencia. Finalmente existe una postura legalista, desde la cual, un delito informático es aquel que el legislador ha catalogado como tal dentro de la ley penal.

Finalmente, el autor Miguel Davara Rodríguez define el delito informático de la siguiente manera:

> "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 (…) Nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General" (Davara, 2008, pág. 358).

Asimismo, debe manifestarse que existen una serie de términos genéricos para nombrar a este tipo de actos ilícitos, entre los que se encuentran: delito informático, delincuencia informática, cibercrimen, delito cibernético, ciberdelito, criminalidad informática, etc. pero todas designan al delito informático como el conjunto de conductas ilícitas.

4.2 Sujetos de la infracción y bien jurídico protegido

Al igual que en cualquier tipo de los delitos, los delitos informáticos presentan dos sujetos del delito: uno activo y otro pasivo, sin embargo, en este tipo de infracciones penales se presentan algunas particularidades que son necesarias de analizar, para posteriormente señalar los aspectos más importantes del bien jurídico protegido.

Partiendo de la idea universal de que el sujeto activo del delito es la persona que lo comete, debe señalarse que, en este caso, se trata de una persona que tiene conocimientos informáticos y que, mediante la utilización de un computador, realiza un conjunto de acciones que implican el cometimiento de un delito que puede afectar a una o varios personas, naturales o jurídicas, e inclusive entidades gubernamentales. En este sentido, el autor Santiago Acurio explica lo siguiente;

> "Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos" (Acurio, 2006, pág. 15).

Según señala el autor, la característica en común de los sujetos activos de la infracción del delito informático, es su habilidad para dominar esta clase de sistemas, y agrega que la mayoría suelen trabajar en alguna actividad relacionada con esta actividad, inclusive se ha llegado a confirmar que la gran mayoría de delitos que sufren las empresas, son ocasionadas por sus mismos empleados.

En lo que se refiere al sujeto pasivo de la infracción de los delitos informáticos, como ya se ha dejado apuntado, son aquellos que sufren de manera directa las consecuencias del delito, y entre éstas se encuentran tanto personas naturales como jurídicas. Respecto de las mismas, el mismo autor el autor Santiago Acurio explica que "En el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones creditícias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros" (Acurio, 2006, pág. 18).

Según explica el autor, los sujetos pasivos del delito van desde personas naturales, hasta organismos gubernamentales, quienes sufren la afectación de distintos bienes jurídicos protegidos por la ley. En este sentido, el autor además recuerda que existe una diferencia conceptual entre sujeto pasivo del delito y víctima, ya que esta segunda categoría es mucho más amplia, pues son aquellas personas que reciben una afectación indirecta por parte del delito.

En el caso del bien jurídico protegido, debe resaltarse nuevamente que los delitos informáticos constituyen una serie de conductas que coinciden con varias figuras penales tradicionales, razón por la cual, no existe un solo bien jurídico protegido afectado, sino que son distintos de acuerdo con la naturaleza jurídica de la acción cometida, de esta manera, en criterio de los autores Claudio Magliona y Macarena López, se tratan de delitos pluriofensivos o complejos, que son definidos por el autor Alfonso reyes como aquellos que "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo" (Reyes, 1981, pág. 76).

Pese a la amplitud de bienes jurídicos que pueden afectar estos delitos, conviene señalar cuales son los más comunes, para lo cual se debe empezar por la información, pues este es uno de los bienes jurídicos que mayormente se afecta a través de estas infracciones, pero muchas veces, la información personal obtenida por el infractor, sirve además para el cometimiento de otros ilícitos que pueden ser patrimoniales.

Precisamente, en cuanto a los bienes jurídicos económicos afectados, son principalmente el patrimonio y propiedad; mientras que, en el caso de la información, también se afecta el derecho a la intimidad y confidencialidad de los datos y la seguridad o fiabilidad del tráfico jurídico y probatorio la reserva. También la afectación sobre la información puede recaer en la afectación de otros delitos más graves contra la integridad física, psicológica y sexual de la persona.

4.3 Características

De acuerdo con las definiciones antes expuestas, así como de los elementos de este delito, ya se puede intuir cuales son algunas de sus características; siendo diversos los autores que señalan un conjunto específico de las mismas. En este sentido, se tomará como punto de partida, las ideas del autor Julio Téllez Valdés, quien enlista las siguientes:

> "1. Son conductas criminales de cuello blanco (*white collar crime*), en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
>
> 2. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
>
> 3. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
>
> 4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

> 5. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
>
> 6. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
>
> 7. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
>
> 8. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
>
> 9. Tienden a proliferar cada vez más, por lo que requieren una urgente regula" (Téllez, 2003, pág. 8)

La primera característica que señala el autor, es la especialidad que tiene los mismos, ya que se necesita de un cierto conocimiento por parte del infractor para su cometimiento, pues no todas las personas están en la posibilidad de adquirir la destreza necesaria para cometer el delito. Por esta misma razón, el autor considera que la segunda característica es que se trata de un delito ocupacional, pues muchas veces al interior del núcleo laboral del criminal, es donde se cometen estos delitos.

Dos de las características señaladas además tienen que ver con los medios con los que se realizan estas infracciones, ya que se tratan de delitos de oportunidad que aprovechan las ventajas que ofrece el mundo digital para delinquir, como la inmediatez de la información y el gran número de posibilidades que existen para escoger a una víctima, debido a las gigantescas redes de información que mantiene estos delitos.

En cuanto a las afectaciones que poseen, el autor considera que los delitos informáticos se realizan principalmente, con el objetivo de afectar al patrimonio de sujeto pasivo, por lo que la finalidad del mismo es económica; aunque también suelen producirse en contra las plataformas informáticas estatales y de los sistemas de defensa.

Así también las ultimas características se encuentran relacionadas, ya que se refieren al marco legal que regula las mismas, que en la gran mayoría de casos no es adecuada ni tutela todas las formas de este tipo de delito. Esta situación también se presenta en el ámbito procesal, ya que, siendo infracciones de carácter altamente técnico, resultan difícil de probar y por lo tanto de sancionar a los infractores. Finalmente, este conjunto de aspectos ha provocado que el delito haya proliferado en todo el mundo y se ha aumentado considerablemente el número de infracciones cometidas.

Por su parte, el autor Marcelo Temperini, considera que existen siete características, siendo la primera de éstas el ser delitos de cuello blanco; sin embargo, el autor considera que en la actualidad esta característica es poco exacta, debido a que la masificación de la información dentro del mismo internet, ha permitido que casi cualquier persona pueda aprender lo

necesario como para cometer un delito informático, de allí que se requiera cada vez menos especialidad del sujeto activo (Temperini, 2018).

La segunda característica de los delitos informáticos es la transnacionalidad, ya que este delito permite que el delincuente este muy alejado de la víctima, inclusive en otro país, de allí que se considere que esta clase de infracciones no reconozca las fronteras geográficas, pues se desarrolla en su mismo universo ilimitado. En criterio del mismo autor, esto también significa una desventaja para la persecución del delito, pues las instituciones de persecución criminal si obedecen a una lógica de territorialidad, requiriéndose de cooperación internacional para poder sancionar a los infractores. Esto sin duda es una ventaja para el delincuente, quien escoge aciertos países para delinquir, donde no existe legislación que permita sancionarlo y así quedar en la impunidad (Ibídem).

En cuanto a la tercera característica, la misma es que se tratan de delitos instantáneos, en razón de que la misma tecnología ofrece la ventaja de que los datos puedan viajar a una velocidad extremadamente rápida, por lo que también esto influye en la dificultad de su persecución.

La cuarta característica del delito, también se hereda de las características de las TICs, pues se tratan de delitos masivos, ya que no solamente en la actualidad existe una gigantesca base de datos en el internet, sino que los mismos están enlazados entre sí, dando la posibilidad de que la persona pueda cometer una misma infracción en contra de varias personas al mismo tiempo.

Como quinta característica se encuentra el anonimato, y en este sentido el autor Marcelo Temperini explica que:

> “Con esta característica nos referimos a la posibilidad de lograr distintos niveles de anonimato que presentan las nuevas tecnologías. Es decir que la persona que las utiliza pueda ocultar su verdadera identidad, o en el caso de las redes, la verdadera conexión desde la cual está llevando adelante sus acciones” (Temperini, 2018, pág. 64).

Esta característica también es una de las que más incide en la investigación del delito, ya que el cometimiento de un delito o varios, puede realizarse de una manera totalmente anónima, siendo más difícil de identificarse la identidad del infractor, por lo que la investigación y sanción del delito tiene una mayor dificultad.

La sexta característica es que se tratan de delitos pluriofensivos, esto debido a que se trata de un conjunto de figuras típicas, lo que ocasiona que las mismas puedan vulnerar a distintos bienes jurídicos protegidos, y aunque principalmente suelen afectar el patrimonio económico

de la persona o entidad, también afectan a otro conjunto de bienes como la seguridad, la integridad física y sexual, la información personal, entre otros.

En cuanto a la última característica, el autor considera que se traten de delitos de investigación compleja, y al respecto señala que:

> "La combinación de varios de los aspectos de las nuevas tecnologías ya desarrollados hasta el momento tienen como consecuencia generar una investigación penal mucho más compleja que las tradicionales. Implica que las fuerzas de seguridad a cargo de dichas tareas tengan un mínimo de conocimientos técnicos, suficientes para comprender las maniobras delictivas y poder llevar adelante una investigación eficaz. La investigación de los delitos informáticos estará marcada por la volatilidad de la evidencia digital, por lo que las fuerzas de seguridad deberán estar adecuadamente capacitadas para lograr una identificación, recolección y preservación de los datos, que deberá hacerse de acuerdo a las buenas prácticas internacionales -y en algunos casos, a protocolos o guías nacionales-, garantizándose la cadena de custodia de todos los elementos que vayan a ser incorporados a la causa como prueba" (Temperini, 2018, pág. 67).

En la referencia expuesta se nota como varias de las características antes señaladas, tiene como consecuencia, que la investigación de este tipo de delitos se muy compleja, de allí que se requiere de un marco normativo adecuado y también de personal altamente capacitados en la investigación de estos delitos, pues de ello dependerá que los mismos sean sancionados de manera adecuada.

4.4 Categorización del ciberdelito

Como se mencionó anteriormente el delito común está tipificado y existe en el ordenamiento jurídico de los Estados, y en razón de que se afectan a distintos bienes jurídicos, este tipo de delitos se ha clasificado de distinta manera y obedeciendo a distintos criterios, de allí que se requiera analizar cada uno de estos de manera breve. Es así que existen un sin número de clasificaciones para los diversos tipos de ilícitos, todo dependerá del enfoque con que cada una de las legislaciones o de los criterios doctrinarios se tenga.

Para Molina Salgado (2003), los delitos informáticos se clasifican de la siguiente manera:

- Como medio o instrumento: Se categorizan las computadoras como método o medio en el cometido del ilícito.
- Como fin u objetivo: Cuando la infracción va dirigida en contra de computadores, accesorios o programas.

Atendiendo a la triada de los principios de la seguridad de la información, se tiene:

- Delitos contra la confidencialidad: Tenemos el espionaje informático, acceso ilícito a un sistema.
- Delitos contra la integridad: Daño premeditado a hardware o software, manipulación de información.
- Delitos contra la disponibilidad: Negación de servicios.

Otra clasificación, es la destinada a proteger el conocimiento, la integridad física y patrimonial de las personas, y son:

- Delitos contra el patrimonio: el fraude informático.
- Delitos de pornografía infantil: relacionados con la violencia sexual, explotación trata de personas que se han llevado a cabo por medio de tecnologías TICs.
- Delitos contra la propiedad intelectual

En el Décimo Congreso de las Naciones Unidas (2010), se menciona que son considerados delitos en las redes electrónicas el espionaje industrial, el sabotaje de sistemas de computación, sabotaje y vandalismo de datos, pesca de claves secretas, estratagemas. La diversidad de delitos informáticos está limitada a tres factores: la imaginación del autor, su capacidad técnica y a deficiencias de los sistemas informáticos. Existe una gran diversidad de delitos cibernéticos, por ello se los ha agrupado en 5 grupos para estudiarlos de mejor manera.

4.4.1 Fraude electrónico

El primer grupo de delitos informáticos, son aquellas que se enmarcan dentro de la conducta de fraude electrónico, mismo que es definido por al autor Alejandro Rodríguez como “la conducta desplegada por un tercero ajeno al titular del medio electrónico de pago, no autorizada ni consentida por este, por conductos electrónicos y que le causa un perjuicio” (Rodríguez, 2014, pág. 290).

Al igual que desde la perspectiva clásica de este delito, el fraude electrónico afecta directamente al patrimonio económico de las personas, solo que, en este caso, la conducta se materializa a través de medios digitales, mediante los cuales el infractor se apodera de cualquier medio de pago, sin autorización del titular, por lo que le ocasiona algún perjuicio.

En esta misma línea de pensamiento se encuentra el autor Andrés Mariño, quien define al fraude electrónico:

> “Como el escenario en el que un tercero se apropia de los datos de identificación de la tarjeta de crédito [o de cualquier medio electrónico de pago individual] y de su titular y, empleando los

> mismos, celebra contratos a distancia por medios electrónicos, telefónicos o telemáticos" (Mariño, 2003, pág. 134).

Nuevamente en la definición presentada por el autor se comprende que el fraude electrónico deriva en una afectación económica a la víctima, de la cual se apropian documentos crediticios o contractuales, con el objetivo de ilícitamente y sin autorización, realizar transacciones económicas en su nombre.

En cuanto a los medios que son utilizados dentro de esta forma de estafa, los mismos pueden ser diversos, pero principalmente se refieren a tarjetas de crédito o debido, pero también a las transacciones de banca electrónica, identificándose dos conductas que componen estos delitos, por un lado, la intercepción de la información del sujeto pasivo, y por otro, la utilización de la información en dispositivos falsos o adulterados.

Este tipo de delito informático tiene variadas opciones de las que se valen los delincuentes para cometer este tipo de infracciones, que serán analizadas de manera individual a continuación.

4.4.1.1 Estafas en banca electrónica (Pishing):

El phishing "es un mecanismo criminal que emplea ingeniería social y artificios técnicos para robar datos de identidad personal de los consumidores y credenciales de cuentas financieras" (Anti-Phishing Working Group, 2019, pág. 2), y como su denominación lo sugiere, es el tipo de estafa que se centra en aspectos relacionados con los bancos, siendo la finalidad del delincuente, el apropiarse de las cuentas de los clientes con el objetivo de ocasionarles un perjuicio económico de las mismas.

Por su parte, AndalucíaCERT realiza una definición mucho más amplia acerca de este delito, en los siguientes términos:

> "El término Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como puede ser una contraseña, información bancaria u otra información personal de la víctima. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial, por lo general utilizando el correo electrónico o mensajería instantánea. Sin embargo, el canal de contacto para llevar a cabo estos delitos no se limita exclusivamente al correo electrónico, sino que también es posible realizar ataques de phishing a través de SMS, conocido como smishing, o de telefonía IP, conocido como vishing" (AndalucíaCERT , 2017, pág. 3).

Según lo señalado por este organismo se comprende como el Phishing es un delito especializado en afectar al sistema bancario y a sus usuarios, mediante la captación de sus

credenciales electrónicas, como usuarios y contraseñas, para así obtener el dinero de la víctima, recalcándose que, en la actualidad, este es uno de los delitos informáticos que mayormente se cometen.

En cuanto a la ingeniería social a la que hace referencia el concepto, es la técnica del engaño explotando el lado psíquico y emocional de los individuos. Asimismo, debe señalarse que el *Pishing* va asociado a otras inventivas ilegales como el malware ara llegar a su cometimiento pleno. El *malware* es un *software* malicioso, que proviene del internet y correo electrónico, con la finalidad de sustraer información sensible de la víctima, aunque también debe tomarse en cuenta que este delito puede ser realizado por medio de dispositivos telefónicos, utilizando el mismo mecanismo.

Las recomendaciones generales para la protección de los usuarios frente a estos delitos es el no abrir ni mucho menos responder a correos de origen desconocido, verificar la dirección exacta de la página en el navegador, no suministrar datos personales a través de mails o sitios web sospechosos.

4.4.1.2 Fraudes en medios de pago físico

En esta subcategoría encontramos el *Card no present fraud*, ocurre cuando el delincuente realiza transacciones en las que no se requiere presentar la tarjeta de crédito o débito del usuario, sino que únicamente debe conocer el número de cuenta, código de seguridad y fecha de vencimiento de la misma, al proporcionar esta información fiable; la transacción se lleva a cabo de forma licita como si fuera realizada por el titular. Generalmente, ocurre por medio de llamadas telefónicas y compras por internet.

Otra infracción, que consiste en un fraude en los medios de pagos físicos es el *skimming,* mismo que tiene como propósito robar la información contenida en la banda magnética y luego realizar una clonación de la tarjeta, con lo cual se tiene acceso a estos medios electrónicos de pago de las víctimas. Para el cometimiento de estas conductas se emplean dispositivos como lectores magnéticos y mini cámaras.

4.4.1.3 Otros tipos de fraudes en la red

La conocida Carta Nigeriana, es un correo electrónico, hace mención que el remitente se ha hecho acreedor a una herencia, y por diversos motivos no se la puede acreditar directamente; es ahí cuando apela al destinatario del correo que le ayude para recibir este dinero en su

cuenta, y como retribución recibirá un porcentaje del mismo. Lo que implica que los estafadores le soliciten información de sus datos bancarios. Muchas de las veces para hacer más creíble su historia, los correos incluyen enlaces de noticias de personas que han sufrido accidentes, o de países con graves crisis sociales o políticas.

Cada vez son más las personas perjudicadas por las estafas conocidas como premio de la lotería. Consiste en enviar un correo electrónico comunicando que usted ha sido acreedor a un millonario premio de lotería extranjera o unas vacaciones de lujo, y para cobrarlo es necesario depositar cierta cantidad de dinero a un consorcio para cubrir gastos de transferencia o proporcionar información personal, y así puede recibir lo ganado. Lo que lo convierte en potencial víctima de robo de identidad y uso fraudulento de su cuenta bancaria.

Ser responsables a la hora de realizar transacciones financieras en línea, tener una cultura preventiva como revisar periódicamente el estado de cuenta, cambiar de contraseñas cada cierto tiempo, no compartir datos con personas que no sean de nuestra confianza e ir a sitios seguros, puede reducir la probabilidad de ser víctimas de fraude electrónico.

4.4.2 Daños informáticos

De manera general se puede afirmar que los daños informáticos, son delitos en los que se emplea *software* diseñado para acceder ilegalmente a un sistema informático, con el propósito de ocasionar daños al equipo, utilizar la unidad para cometer otro tipo de delitos, o para robar información.

Respecto a los delitos de daños informáticos, el autor Julio Mazuelos los define de la siguiente manera:

> "El delito de daños informáticos o también denominado sabotaje informático persigue la sanción de quien perturba un procesador de datos que es de esencial importancia para una empresa ajena o para una autoridad, a través del menoscabo, destrucción, deterioro, inutilización, eliminación o transformación de un equipo de procesamiento de datos o un soporte de datos. La configuración de un tipo penal especial de daños se fundamentaría en la toma de conciencia acerca de la necesidad de un desarrollo del procesamiento de datos libre de perturbaciones, para la economía y la administración pública y, a su vez, en la comprobación de los elevados daños que conlleva esta especial forma peligrosa de sabotaje económico" (Mazuelos, 2007, pág. 29).

De acuerdo con lo señalado por el autor, se comprende como el daño informático, como su denominación lo sugiere, implican la realización de una conducta que afecte la integridad del patrimonio informático, es decir, la eliminación, el deterioro del equipo o principalmente de la

información que se halla en determinada base de datos, pudiendo ser atacada la información de las personas particulares, pero también las empresas y entidades públicas.

Asimismo, dentro de los delitos de daño informático existen un subconjunto de delitos que lo integra y que forman diversos tipos penales, entre los que se encuentran principalmente: las bombas lógicas, los gusanos, los virus informáticos, malware, ciberterrorismo, ataques de denegación de servicio, Bombardeo de Correo Electrónico, manipulación de programas, Manipulación de los datos de salida, entre otros.

4.4.3 Propiedad intelectual

Al igual que otras figuras típicas antes ya señaladas, los delitos contra la propiedad intelectual siempre tuvieron formas de afectación relacionadas con la falta de autorización del titular para el uso de las mismas; sin embargo, este tipo de delitos ha tenido una mayor potenciación debido al desarrollo de las TICs, ya que debido a la facilidad con la que se comparte la información dentro del internet, se hace casi imposible realizar un control real de las creaciones artísticas, literarias o derechos de propiedad industrial que existen en el ciberespacio.

En cuanto a la definición misma de los delitos contra la propiedad intelectual, el autor Miguel Díaz afirma que:

> "En diversos delitos contra la propiedad intelectual e industrial se establece como requisito típico expreso la ausencia de consentimiento o autorización del titular del correspondiente derecho de propiedad intelectual. Tal consentimiento o autorización operará a menudo como causa de justificación, excluyendo por tanto toda clase de ilicitud y no sólo el injusto penal del hecho. Sin embargo, en otras ocasiones es posible que sólo excluya éste, encontrándonos ante una causa de exclusión de la tipicidad penal que dejaría subsistente la ilicitud derivada de las normas no penales sobre propiedad intelectual e industrial" (Díaz, 2009, pág. 101).

En los delitos informáticos de propiedad intelectual, el bien jurídico afectado es el mismo, es decir, la propiedad de la persona, ya que se usa sin justificación y consentimiento alguno de los autores su propiedad que está registrada de acuerdo a la normativa nacional o internacional, siempre que la misma se realice por medios informáticos.

En cuanto a las principales figuras de tipos penales informáticos en contra de la propiedad intelectual, los más importantes son la Infracción del *copyright* de bases de datos y la infracción de los conceptos de copia, distribución, sección y comunicación pública de contenidos de autor que son ilegalmente utilizados dentro del sistema informático.

No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual, el propietario del sistema permite que los usuarios hagan "*downloads* " de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

4.4.4 Delitos relacionados con la distribución de contenido

Los delitos relacionados con la distribución de contenido, tienen como principal objetivo, el envío de material prohibido por la legislación, estando relacionados los mismos de manera principal con la pornografía infantil y su distribución, así como el envío de pornografía a niñas, niños o adolescentes, situación que debe producirse, al igual que los anteriores casos, mediante un soporte electrónico o informático.

Precisamente, respecto de la Pornografía Infantil, los autores Rodolfo Estrada Posada y Roberto Somellera afirman lo siguiente:

> "Pornografía Infantil: Este es un crimen que está claro que es ilegal, ya sea en Internet o fuera de él. Algunos operativos han logrado detener a los delincuentes, pero todavía hay manera de obtener imágenes de niños con poca ropa o en diferentes actos sexuales. En materia legal, la gente que usa o provee de pornografía infantil, enfrentan los mismos cargos, ya sea que la fotografía este digitalizada o en un pedazo de papel fotográfico. En los juicios de los usuarios de ese material que fueron arrestados recientemente por el FBI, retarán la validez de las leyes, en cuanto se apliquen a los servicios en línea" (Estrada & Somellera, 1998, pág. 430).

En cuanto a la protección del bien jurídico de este tipo de delitos, el mismo es la integridad sexual de los menores, pues ya sea que el material pornográfico se le muestra a niñas, niños o adolescentes, o que en el mismo participen cualquiera de ellos, esto constituye una clara afectación de este bien jurídico, de allí que el legislador le haya concedido una protección jurídica, sancionando a los infractores que guarden, almacenen, produzcan o distribuyan por medios electrónicos este tipo de material.

4.4.5 Otros ciberdelitos

4.4.5.1 Ciberacoso

Para comprender el alcance de este delito, debe tomarse en cuenta los distintos tipos de acoso que existen, pues las mismas formas de casos que se producen de manera personal, son realizadas a través de los medios electrónicos, y asimismo vulneran un conjunto de bienes jurídicos entre ellos el de la libertad personal, sexual o psicológica de la persona.

El ciberacoso, casi siempre se lo ha relacionado con el contexto escolar de las personas, sin que medie una intención sexual en la misma, pues en este caso se estaría haciendo referencia la figura del *Grooming.* En este sentido, la autora Mara Resio considera que los medios informáticos, han bridado una mayor oportunidad a los infractores para que comentan este tipo de conductas, y así explica que

> "El medio digital, por sus características técnicas y el anonimato que confiere a sus usuarios, también brinda un espacio de oportunidad favorable al incremento de conductas inapropiadas, disvaliosas e incluso delictivas. (…) los ciberacosos, hostigamientos, amenazas y extorsiones, que encuentran en este entorno digital el ambiente propicio para llegar en menor tiempo a un número mayor e indeterminado de víctimas" (Resio, 2018, pág. 124)

En este sentido, Guillermo Cárdenas señala que las conductas como el *bullying*, que consisten en "toda agresión deliberada que un individuo o grupo ejerce sobre alguien de manera reiterada y sistemática", cuando dicho hostigamiento se realiza a través de "los medios digitales mediante mensajes de correo electrónico o de teléfono celular, blogs y redes sociales, entonces se considera acoso cibernético" (Cárdenas, 2015, pág. 11).

4.4.5.2 Grooming

Esta figura constituye un tipo de acoso que se presenta exclusivamente en el plano sexual, e implica que una persona, generalmente mayor de edad, acose a un menor de edad, mediante los medios electrónicos, siendo una de las figuras típicas que se crearon con la existencia de las TICs.

En cuanto a la definición de esta nueva figura penal, la autora Mara Resio hace la siguiente explicación:

> "Ciberacoso sexual o "grooming", "que abarca conductas tendientes a contactar por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual" (Resio, 2018, pág. 122)

Como se observa de a definición realizada, el *grooming*, además de ser por sí mismo un delito, constituye un tipo penal que busca la consumación de un segundo tipo penal que atente en contra de la libertad o integridad sexual de la persona, siendo las víctimas los menores de edad.

5 CONSIDERACIONES ACERCA DEL PERITO INFORMÁTICO

5.1 Perito informático

El Derecho y las Tecnologías de Información y Comunicaciones (TIC), son disciplinas que pertenecen a ámbitos distintos, el primero estudia la regulación de la conducta humana en la sociedad; y las segundas son un conjunto de servicios, aplicaciones y herramientas tecnológicas que van cobrando mayor relevancia a la hora de acceder a la información y al conocimiento en todos los ámbitos de la vida moderna. Sin embargo, estas nuevas tecnologías son utilizadas para cometer delitos, tal es el caso de robos, extorsiones, fraudes y otros tipos de hechos ilícitos a través de los medios electrónicos.

De ahí nace la necesidad de contar con personas que tengan la experticia para buscar las evidencias que contribuyan a sancionar estos delitos, este profesional es conocido como Perito informático. Son los encargados de recolectar, preservar, analizar y presentar datos que han sido procesados de forma electrónica y almacenados de forma digital. Su principal objetivo es dar respuesta a preguntas básicas: qué se ha alterado, cómo y quién ha sido el responsable. El perito debe ser imparcial, no cometer hecho con dolo, imprudencia o falta de celo al realizar la pericial. Al mismo tiempo, sus aptitudes deben estar avaladas por una institución reconocida. Esto impedirá que la validez de las evidencias sea puesta en entredicho.

Cada país contempla una serie de requisitos en función a sus estudios, formación, experiencia y en algunos casos se exige contar con certificaciones específicas, para que un perito pueda ser reconocido y posteriormente pueda realizar su labor, sin embargo, debe destacarse que en lo que se refiere a la investigación criminológica del delito informático en sí mismo, existen algunos retrasos y deficiencias normativas que requerirían ser subsanadas, para de esta manera proteger de manera adecuada a las personas frente a estos hechos delictivos.

5.2 Normativa jurídica relacionada al quehacer del perito informático

La aplicación de una normativa que sancione actos realizados en el ciberespacio, tiene sus complejidades, debido a que no tiene límites políticos ni un espacio físico. Marc Goodman (2016) define al ciberespacio diciendo que “se trata de un ambiente intangible; no es un mundo de átomos y células, sino digital. Los bytes no tienen peso, olor ni color y viajan a la velocidad

de la luz" (p. 28). Sin embargo, todos los actos realizados a través del ciberespacio no deben vulnerar los derechos de las personas.

Cuando se produce un acto ilícito, en el ámbito jurídico, es fundamental determinar el lugar de origen, debido a que esto si se ha cometido dentro de un espacio territorial en el cual existen normas que rigen el Estado, promulgadas de manera correcta por los legislativos, que sancionan a esta conducta como un delito, se podrá sancionar al infractor; mientras que en el caso de que no se tipifique este acto como un delito, se requerirá de la asistencia y cooperación internacional a fin de poder sancionar al responsable, aplicando para ello las normas comunitarias regionales o del derecho internacional público, dependiendo del país en concreto.

También, existen ocasiones en las que el cometimiento de delitos informáticos involucra a más de un Estado, es por ello que el perito informático debe conocer la normativa en materia de cooperación internacional o asistencia jurídica mutua, (la misma que se explicará más adelante), pues de ello dependerá que se pueda determinar la existencia material del delito y sancionar al infractor.

El conocimiento de las normas que rigen la actividad del perito también resulta de gran importancia, debido a que en muchos países no existe normativa nacional o comunitaria regional que regule aspectos en concreto respecto de las actividades que deberá realizar el perito informático, de modo que, al conocer las legislaciones internacionales, podrá tener una visión más amplia y mejores conocimientos acerca de su labor.

Precisamente esta situación puede observarse en gran parte de Sudamérica, y concretamente en Ecuador, donde muchas de las infracciones informáticas no han sido tipificadas, así como gran parte de los protocolos de investigación no se encuentran actualizados o muchas veces son inexistentes, situación que se replica dentro del organismo regional al que pertenece, que es la Comunidad Andina de Naciones, (en adelante CAN), que no cuenta con normativa regional para combatir los delitos informáticos mediante la asistencia internacional.

Por estas razones, a continuación, se realizará un análisis comparativo de las distintas legislaciones, aplicando el orden jerárquico de aplicación de las leyes, conocido como pirámide de Kelsen, identificando aquellas normas que regulan la actividad del perito informático, así como también las que prescribe requisitos para desempeñar esta labor.

6 DESCRIPCIÓN DE LA METODOLOGÍA APLICADA

6.1 Introducción a la metodología

Para el desarrollo del presente proyecto de investigación científica, se ha utilizado el modelo exploratorio, ya que este permite caracterizar un fenómeno o situación concreta de estudio, indicando los rasgos más importantes o diferenciadores, con el objetivo de llegar a conocer a profundidad las situaciones, actividades, objetos, procesos y personas que intervienen, que para el presente caso es la información acerca de las leyes y regulaciones relacionadas con el desarrollo de la actividad del perito informático.

Debe señalarse que la meta de este modelo de investigación no se limita a la recolección simple de los datos, sino que en la misma se busca la identificación de las relaciones que existen entre las variables; es decir, en este caso, se buscará realizar un análisis comparativo de las diversas normas, estableciendo coincidencias, diferencias y aportes a fin de obtener importantes concusiones al respecto.

6.1.1 Tipo de investigación

Siendo el objetivo primordial de este método el descomponer un objeto de estudio separando cada una de las partes del todo para estudiarlas de forma individual, a través del mismo se pretende analizar cada uno de los ordenamientos jurídicos de cada país a fin de establecer cuáles son las normas aplicables que regulan la actividad del perito informático, de modo que se requiere analizar por separado cada una de estas normas, para al final obtener una conclusión global de cada ordenamiento, pues solo así se podrá realizar el correcto estudio del marco normativo.

Método Descriptivo.- Mediante el método descriptivo, que se comprende como aquel que busca aplicar una investigación sistemática y como se desarrolla un fenómeno, mediante su descripción e interpretación de las condiciones que se dan en una situación y momento determinado, se pretende realizar una visión general de la actividad del perito informático, para lo cual se pretende describir la situación normativa de los delitos informáticos que existente para sancionar este tipo de delitos, ya que únicamente cuando se haya analizado esta situación, se podrá contextualizar de manera correcta la actividad del perito en su campo.

Método hermenéutico comparativo.- La hermenéutica, comprendido como la actividad destinada a la interpretación y análisis de fondo de las normas jurídicas, se requiere al momento de realizar un análisis normativo de una legislación nacional o extranjera, de manera

que esta método será la base para establecer una correcta comparación de las legislaciones que regulan la actividad del perito informativo, pues solo de esta manera se podrá identificar las fortalezas y las deficiencias de las mismas, con el objetivo de plantear mejoras y avanzar hacia una universalización de la investigación de los delitos informáticos, cuya cometimiento es también global.

6.1.2 Técnica de recopilación de información

En cuanto a las técnicas de investigación, al tratarse de un modelo de carácter estrictamente documental, las técnicas a aplicarse será el análisis de contenido a fondo, pues se requerirá del estudio de la documentación relacionada con los delitos informáticos, pero además de las leyes que regulan la actividad del perito informático en su campo de trabajo, que son eminentemente de tipo criminalística.

6.1.3 Modalidad de la investigación

La investigación a desarrollar es documental, para ello se procedió con la lectura de material bibliográfico relacionado con la temática de la investigación, que tenga un contenido científico adecuado e información de calidad, que en este caso se encuentran en libros, publicaciones de revistas científicas, *papers*, tesis de doctorado, páginas web, portales institucionales de organismos criminológicos de cada Estado, bases de datos, registros o boletines oficiales donde consten la normativa de cada país.

Del mismo modo, se analiza la normativa legal que rige España, Ecuador y varios países de distintas regiones, con el objeto de identificar los vacíos legales existentes y los aportes que se pueden brindar.

6.2 Legislación comparada

Dentro del contexto latinoamericano, y principalmente dentro de la legislación ecuatoriana, los protocolos de investigación del delito a través de las distintas disciplinas científicas que componen la criminalística, no han sido desarrollados de manera eficaz y de acuerdo con los estándares de investigación científica internacional que se requieren para la efectividad de este proceso.

De hecho, se puede observar que en lo que se refiere a los protocolos de investigación del delito, los mismos han sido incorporados de manera reciente, ya que con anterioridad a la vigencia del Código Orgánico Integral Penal del año 2014, la actividad criminológica era desarrollada de manera exclusiva por los agentes policiales, concretamente por una rama de la Policía Nacional del Ecuador, denominada Policía Judicial, que inclusive hasta los días actuales realiza la investigación del delito en gran parte del territorio nacional.

Este organismo, carecía de gran parte de protocolos y manuales técnicos de actuación en las distintas disciplinas de la investigación del delito, e inclusive de personal capacitado en estas áreas, siendo sus reglamentos de actuación, principalmente normativo - jurídicos, sin seguirse las recomendaciones más básicas de organismos internacionales como la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC).

Si bien es cierto, con la promulgación del Código Orgánico Integral Penal se crea un organismo criminalístico de investigación del delito compuesto en gran parte por personal civil, aunque también por personal policial, bajo la denominación de "Sistema especializado integral de investigación, de medicina legal y ciencias forenses", el mismo todavía no cuenta con todos los protocolos técnicos de investigación del delito, ya que apenas en el año 2014 se promulgaron los Manuales, protocolos, instructivos y formatos del sistema especializado integral de investigación medicina legal y ciencias forenses, en los cuales se determinan estándares mínimos de actuación criminológica, aunque no en todos los campos de investigación del delito.

Es así, que en lo que se refiere a las pericias de investigación de delitos informáticos, no existe un protocolo de actuación idóneo, pese a la gran importancia que tiene la investigación de estos delitos en la actualidad, que se han incrementado de manera considerable en el Ecuador y en también en todo el mundo.

Esta situación que ocurre en el Ecuador, contrasta con algunos países de la Región (Como Colombia, México, Argentina), que disponen de instrumentos de investigación de los delitos informáticos de acuerdo con los estándares internacionales, lo que permite una eficiencia en la investigación del delito, de allí que debe tomarse en consideración los aportes que pueden tener los mismo para la plena capacitación del perito informático en el Ecuador.

Precisamente, ante este déficit, la propuesta de la presente investigación se sustenta en la necesidad que existe de realizar un análisis de derecho comparado entre las distintas normativas que regulan la actividad del perito informático dentro de diez países, con el objeto de analizar las fortalezas y debilidades de estos instrumentos normativos en la investigación de delitos informáticos.

Ya que desde la doctrina se ha señalado los aspectos más importantes relacionados el delito informático, y con la investigación de estos delitos, así como también aquellos estándares mínimos a través de los cuales se puede realizar la investigación criminológica técnica, cumpliendo con los principios del debido proceso y la validez probatoria, se requiere establecer el marco normativo de la actividad pericial dentro de países altamente capacitados en investigación pericial informática, para compararlas con la normativa ecuatoriana, y de esta manera poder subsanar aquellas deficiencias que existan en el Ecuador.

La propuesta de comparación normativa, tomará en cuenta la comparación de las principales áreas de los protocolos de investigación del delito, a fin de establecer los vacíos legales que pudieran presentarse en una u otra norma, creando un protocolo modelo idóneo para la investigación de delitos informáticos, que pudiere orientar la actuación del perito informático en el Ecuador, ante la deficiencia de la normativa local.

Además, este modelo podría servir a futuro para consolidarse como un instrumento de aplicación de investigación criminológica a nivel regional, pues al tomar en cuenta los aspectos técnicos y estándares mundiales, subsanando los vacíos legales de cada legislación, el mismo pudiere servir de base para la coordinación de investigación dentro de la Comunidad Andina de Naciones, que tampoco cuenta con un instrumento estandarizado de investigación de delitos informáticos transnacionales, que ayude en la coordinación de las fiscalías de los países miembros.

6.2.1 Legislación española

La legislación española presenta una jerarquía consolidada por leyes y normas que son elaboradas por los poderes del Estado. De acuerdo con lo dispuesto en el artículo 1.2 del Código Civil, las normas inferiores que contradigan a las superiores carecerán de validez, siendo la norma más importante la Constitución Española que rige desde su publicación en el Boletín Oficial del Estado el 29 de diciembre de 1978.

En lo que se refiere a la normativa constitucional, siendo la base sobre la cual se disponen un conjunto de derechos de la persona, algunas hacen referencia al derecho a la tutela efectiva y también a los derechos que forman parte del debido proceso, en el cual, se abordan aspectos acerca de la prueba de manera general, y no de manera específica en la prueba pericial. Es así que el artículo 24 dispone:

> "Artículo 241. Todas las personas tienen derecho a obtener tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda

> producirse indefen-sión.2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia (…)".

La Constitución Española dispone el derecho que tiene todas las personas para que, en los distintos procedimientos judiciales, incluyendo los de carácter penal, puedan hacer uso de los medios de prueba respectivos para ejercer el derecho a la defensa técnica, entre los que se encuentran la prueba pericial.

Además, la Constitución española reconoce la plena vigencia de los Tratados internacionales y el Derecho comunitario de la Unión Europea como parte de su normativa, de allí que todos los instrumentos y protocolos que sean expedidos que tengan como finalidad, la lucha contra los delitos informáticos, son de obligatorio cumplimiento para España. Estos tratados serán analizados más adelante.

En lo que se refiere a los delitos informáticos que se hallan contemplados dentro de la legislación española, los mismos no se hallan previstos dentro de un solo título, sino que, al contrario, los mismos están ubicados de acuerdo al bien jurídico que afectan

Así, dentro del Título VIII que se refiere a los Delitos contra la libertad e indemnidad sexuales, está el artículo 183ter, está tipificado el delito de grooming. En el Título X, de los Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, el artículo 197 sanciona a quienes se apoderen utilicen o modifiquen los datos reservados personales o familiares contenidos en soportes informáticos.

En el Título XIII: Delitos contra el patrimonio y contra el orden socioeconómico, se encuentra cuatro delitos informáticos, siendo el primero el previsto en el artículo 248, que sanciona la estafa por medios electrónicos. En el artículo 264 se sanciona el delito de daño informático, es decir aquel que se comete en contra de la integridad de las bases de datos.

En el artículo 270 del mismo cuerpo legal, se hace constar los delitos informáticos en contra de la propiedad intelectual, que implican el uso de las obras literarias, artísticas o científicas, pro medios informáticos, sin el debido consentimiento por parte de los legítimos propietarios del mismo. Dentro de los artículos 278 y 279, también se sanciona otro delito informático en contra de la promediad intelectual, en este caso la revelación de los secretos empresariales a través de medios electrónicos.

Finalmente, dentro del Título XXII que se refiere a los delitos contra el orden público, en el artículo 578 hace referencia a los delitos de terrorismo y su exaltación por medios electrónicos,

así como también de desprestigio o menosprecio de las víctimas de terrorismo, que se realicen por medios electrónicos.

Ya en lo que se refiere a la actividad pericial, debe destacarse algunos preceptos de la Ley de Enjuiciamiento Criminal, publicada en el Boletín Oficial del Estado núm. 260, de 17/09/1882m, en cuyo artículo 457 se dispone que:

> "Los peritos pueden ser o no titulares. Son peritos titulares los que tienen título oficial de una ciencia o arte cuyo ejercicio esté reglamentado por la Administración. Son peritos no titulares los que, careciendo de título oficial, tienen, sin embargo, conocimiento o prácticas especiales en alguna ciencia o arte".

Seguidamente, la normativa dispone que el juez deberá escoger a los jueces que tengan título por encima de los que no lo tengan, y dispone cada uno de los aspectos acerca del nombramiento y la forma como se realizarán las distintas pericias dentro del procedimiento penal.

Otra de las normas que regulan la actividad del perito informático dentro de la legislación española es la ley concursal, a través de la cual se procede con la designación de los peritos; la ley de enjuiciamiento civil, en la cual se establecen los requisitos que deberá cumplirse para poder ejercer las pericias en el ámbito informático, y algunas pericias informáticas que también se requieren dentro del ámbito civil; El código de comercio y código civil, en la cual también se designa las diligencias en las cuales se usarán estas pericias dentro de estos mismos campos.

En lo que se refiere a los requisitos para ser perito, los mismos se encuentra establecidos dentro de la Ley de Enjuiciamiento civil, que es la que regula los mayores aspectos relativos a los medios de prueba, incluida la pericia. Precisamente, dentro del artículo 339 se regula la solicitud de designación de peritos y también acerca de los honorarios que percibirá; mientras que dentro del artículo 340 se dispone que "el perito deberá estar en posesión de la titulación oficial relacionada con la materia del dictamen"

En lo que se refiere a las profesiones que debe tener un profesional para ser designado como perito informático, pueden ser: Ingeniero en Informática, Licenciado en Informática, Master en Informática, Ingeniero Técnico en Informática, Diplomado en Informática, Título extranjero equivalente convalidado mediante la ley española.

Un segundo requisito que se dispone dentro de la normativa española, es que quienes quieran ser designados como peritos no podrán haber sido condenados por un delito, es decir, no pueden tener ningún antecedente penal registrado.

Un tercer requisito, es que los profesionales deberán demostrar a la administración que saben peritar, esto implicaría que además de tener un título dentro de la rama informática antes ya señalada, deberán haber adquiero experiencia necesaria, mediante la colegiatura en cursos de peritaje o de criminalística.

En cuanto al cuarto requisito, implica que el perito deberá estar afiliado a alguna de las asociaciones de peritos informáticos o los colegios oficiales de ingeniería informática, ya que esto les permitirá estar disponibles dentro de las listas de peritos a ser escogidos cuando un juzgador lo requiera.

El último requisito tiene que ver con que el profesional deba aprobar las pruebas básicas de acceso a los cuerpos y superar los exámenes de las distintas academias oficiales de los cuerpos antes referidas, ya que solamente una vez que se hayan cumplido con estos últimos pasos se podrá incluirlos en las listas oficiales para que completen las vacantes que pudieren existir.

Como se observa, la legislación española es muy rigurosa al momento de designar a los peritos informáticos, pues existe un conjunto de requisitos que son difíciles de cumplir, no siendo solamente necesario el cumplimiento de requisitos de carácter académico, sino que además deberán acreditar que tiene experiencia en la realización de peritajes y posteriormente superar cada uno de los concursos que les permiten acceder a la colegiatura como peritos.

En este sentido, debe destacarse que la legislación española constituye un ejemplo y modelo a seguir en otros países, principalmente de Sudamérica, en donde no se disponen requisitos tan complejos y sobre todo tan especializados para poder acceder a realizar pericias dentro del campo informático.

6.2.2 Legislación ecuatoriana

En Ecuador, la primera observación que se debe realizar, es de acuerdo con lo previsto dentro de la misma Constitución República del Ecuador, en su artículo 425, la misma es la norma suprema del Estado y prevalece por encima de cualquier norma del ordenamiento jurídico.

Esta Constitución rige desde su publicación en el Registro Oficial No. 449, el 20 de octubre de 2008 y conforme se dispone dentro de su artículo 1, el Ecuador “es un Estado constitucional de derechos y justicia”, razón por la cual el artículo 3, numeral primero, dispone que el deber primordial del Estado es la protección de los derechos de todas las personas, lo que incluye

también el debido proceso, que en la legislación ecuatoriana es concebido como un derecho fundamental.

> "Art. 76.- En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: (…) 4. Las pruebas obtenidas o actuadas con violación de la Constitución o la ley no tendrán validez alguna y carecerán de eficacia probatoria. (…) 7. El derecho de las personas a la defensa incluirá las siguientes garantías: j) Quienes actúen como testigos o peritos estarán obligados a comparecer ante la jueza, juez o autoridad, y a responder al interrogatorio respectivo."

Conforme se dispone dentro de la Constitución ecuatoriana, toda persona tiene derecho a que se le respete el derecho al debido proceso en aquellos procesos en los cuales se resuelvan acerca de sus derechos, lo que incluye el principio de legalidad de la prueba y además la obligación de que se permita la defensa, para lo cual es indispensable que quinees actúen como peritos comparezcan personalmente en el juicio.

En lo que se refiere a la normativa jurídica en materia penal, ha sufrido modificaciones en los últimos años, concretamente en el año 2014, cuando se promulga el Código Orgánico Integral Penal (En adelante COIP), que remplazo al Código Penal y al Código de Procedimiento Penal, no obstante, a diferencia de otras legislaciones como es el caso de la española, existen conductas delictivas que no están tipificadas, y en algunos casos quedan impunes, debido a la falta de conocimiento o herramientas adecuadas para investigar y aplicar la ley para castigar esta clase de infracciones.

Es así que el COIP Es un compendio donde se establece los delitos y las penas conforme al sistema penal ecuatoriano. En la sección tercera. "Delitos contra la seguridad de los activos de los sistemas de información y comunicación", está dedicada a detallar los diversos delitos relacionados con revelación ilegal de bases de datos, intercepción ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

En cuanto a los dos primeros delitos que se han tipificado dentro del COIP, los mismos tienen que ver con la protección de los datos, pues sancionan a la persona que revele o intercepte este tipo de datos sin su debida autorización. Posteriormente, la norma penal sanciona a los delitos que afecten el patrimonio económico. Los siguientes delitos son aquellos que provocan un daño informático.

Otros tipos de delitos informáticos se sancionan en otras secciones del COIP, como en las Diversas formas de explotación, en donde constan los delitos de pornografía infantil con

utilización de niñas, niños o adolescentes y su comercialización. Así también, el fraude informático se encuentra tipificado dentro de los Delitos contra el derecho a la propiedad.

Otras normas en donde se hace referencia a la actividad del perito, pero en campos no penales es el Código Orgánico General de Procesos (en adelante COGEP), que es la normativa que regula entre las partes los procedimientos que se llevan a cabo en los procesos judiciales en materias no penales ni constitucionales.

En cuanto a la normativa que regula los requisitos que deben cumplir los profesionales para ser calificados como peritos, la misma se realiza de manera general hacia todos los profesionales en todas las disciplinas de la ciencia, y no se centra exclusivamente en el perito informático.

Así, el instrumento más importante es el Reglamento del Sistema Pericial, en el cual se establece que los peritos para que puedan participar en los procesos judiciales o pre procesales deben cumplir con los requisitos establecidos en el Reglamento del Sistema Pericial Integral e inscribirse en el Consejo de Judicatura, en el cual se determinó que los profesionales deben ser expertos y contar con al menos dos años de práctica y de experiencia, esto se verificará con la presentación de mínimo 10 informes periciales realizados anteriormente.

Debe manifestarse que con posterioridad se introdujeron Reformas al Reglamento del Sistema Pericial Integral de la Función Judicial: Resolución 040-2014, de 10 de marzo de 2014, mediante la cual el pleno del Consejo de la Judicatura resuelve expedir el Reglamento del Sistema Pericial Integral de la Función Judicial. Posterior sufrió una reforma en algunos artículos el 10 de mayo del 2017. Precisamente dentro de este instrumento jurídico se contemplan los requisitos para poder ser designado como perito, siendo éstos:

> "Art. 4.- Requisitos.- Las personas que deseen calificarse como peritos de la Función Judicial, deben cumplir con los siguientes requisitos: 1. Ser mayores de edad, ser capaces y estar en ejercicio de sus derechos de participación; 2. Ser conocedoras o conocedores y/o expertas o expertos en la profesión, arte, oficio, o actividad para la cual soliciten calificarse; 3. En el caso de profesionales, tener al menos dos (2) años de graduadas o graduados a la fecha de la solicitud de calificación, y cumplir con los requisitos de experiencia establecidos en este reglamento. Para las y los demás expertos tener al menos dos (2) años de práctica y experiencia a la fecha de la solicitud de calificación, en el oficio, arte o actividad en la cual tengan interés de calificarse; Tratándose de profesionales en medicina humana que soliciten su calificación para una especialidad médica, además de los títulos profesionales debidamente inscritos en la Secretaria de Educación Superior, Ciencia, Tecnología e Innovación "SENESCYT", deberán acreditar al menos cinco (5) años de experiencia en la práctica de la respectiva especialidad".

En cuanto a los requisitos dispuestos para que se pueda ejercer la actividad de perito dentro de las distintas áreas, la normativa ecuatoriana es mucho más flexible que la española, pues

solamente dispone que deberán ser personas capacitadas en su área y no también en el campo de la pericia. En cuanto a los años de experiencia, solamente deberán acreditar 2 años en su profesión y 5 en el caso de los profesionales de la salud.

Asimismo, no se dispone una prohibición de ejercer las actividades periciales para quienes tiene antecedentes penales, sino que únicamente que tengan la mayoría de edad y que se deberá estar en ejercicio de los derechos de ciudadanía; esto debido a que la Constitución ecuatoriana prohíbe cualquier forma de discriminación por motivos de pasado judicial, dentro de su artículo 11, numeral 2.

Otros instrumentos que regulan la designación de peritos dentro de los procedimientos panelas, son el Instructivo para Designación de Peritos por Fiscalía, mismo que fue creado a través de la dirección de Asesoría Jurídica mediante el memorando No. 020-DAJ_FGE-2016, expide un Instructivo para designación de peritos por parte de la Fiscalía General del Estado, en la cual se detalla cómo realizar la solicitud de un perito, certificación presupuestaria previa, el correspondiente nombramiento y posesión del perito designado, y finalmente se establece el pago de honorarios periciales. Este instrumento, en cuanto a los requisitos para la designación de peritos se remite al Reglamento del Sistema Pericial Integral de la Función Judicial:

También debe manifestar que existe un sistema de Búsqueda de Peritos: El Consejo de la Judicatura, en su página web oficial tiene un registro de peritos acreditados en diferentes áreas, se tiene que completar uno varios parámetros de búsqueda para que se despliegue un listado con la información relacionada al profesional. Su acreditación tiene vigencia de un periodo de 2 años.

6.2.3 Legislación colombiana

Una vez que se han analizado los dos países que han sido objeto central de la investigación, corresponde analizar un conjunto de países que también tienen jun conjunto de regulaciones acerca de los delitos informáticos y las normas a través de las cuales se podrá realizar la designación de peritos, para lo cual, se ha decidido empezar por los países que forman parte de la CAN, pues son los más próximos a Ecuador, y uno de los grandes vacíos que existe a nivel regional, es precisamente la falta de normativa en la subregión andina respecto de este importante asunto, esto pese a la existencia de normativa vinculante para los Estados en otras áreas, pero en lo que se refiere concretamente al delito informático y la cooperación internacional, no se ha realizado un mayor esfuerzo.

En lo que se refiere a las normas que deberá conocer el perito, las mismas parten con el análisis de la Constitución Política de Colombia, en la cual se ha dispuesto el derecho al debido proceso que deben respetar todas las personas que intervienen en los procedimientos penales, de modo que en la norma suprema colombiana el debido proceso también se le considera como un derecho fundamental de todas las personas, según lo prescribe su artículo 29

> "Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y administrativas. Nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa, ante juez o tribunal competente y con observancia de la plenitud de las formas propias de cada juicio. Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable. Quien sea sindicado tiene derecho a la defensa y a la asistencia de un abogado escogido por él, o de oficio, durante la investigación y el juzgamiento; a un debido proceso público sin dilaciones injustificadas; a presentar pruebas y a controvertir las que se alleguen en su contra; a impugnar la sentencia condenatoria, y a no ser juzgado dos veces por el mismo hecho. Es nula, de pleno derecho, la prueba obtenida con violación del debido proceso."

Dentro de la legislación colombiana, el derecho al debido proceso contempla también un conjunto de derechos, entre los que se encuentra la legalidad de la prueba, ya que todas las pruebas deben ser obtenidas en estricto respeto de los derechos de las personas pues de lo contrario carecerán de eficacia normativa, y estas deberán ser contradichas por su contraparte para que puedan ser aceptadas dentro de los tribunales penales.

En lo que se refiere a los delitos informáticos, se encuentran tipificados dentro del Código Penal colombiano, y al igual que en el caso de las dos legislaciones antes ya referidas, se encuentra agrupadas de acuerdo con el bien jurídico que lesionan las mismas, y no todas en un solo capítulo. Sin embargo, un gran número de las mismas se halla dentro del capítulo VII que se refiere a los delitos de la violación a la intimidad, reserva e interceptación de comunicaciones.

Dentro de este grupo de delitos se encuentra en primer lugar, el conjunto de tipos penales que afecta el derecho a la reserva de la información, es decir, el delito de violación ilícita de comunicaciones, la interceptación de las comunicaciones y la divulgación y empleo de documentos reservados.

Otros delitos que pertenecen a este mismo grupo de delitos son la Violación ilícita de comunicaciones o correspondencia de carácter oficial y la Utilización ilícita de redes de comunicaciones; mientras que dentro de esta misma sección se contempla un delito de daño informático, siendo el acceso abusivo a un sistema informático.

En cambio, dentro del Título IV se encuentran los delitos contra la Libertad, Integridad y Formación Sexuales, en los cuales se tipifican los delitos informáticos en contra del contenido,

y concretamente dentro del artículos 218 está el Pornografía con personas menores de 18 años mientras que en el artículo 219 A se encuentra la Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores.

En el Título VI se encuentra un delito informático que afecta el patrimonio económico de la víctima, siendo este el acceso ilegal o prestación ilegal de los servicios de telecomunicaciones, mientras que los demás se hallan dentro del Título VII bis, que se refiere a la Protección de la información y de los datos, se encuentran un conjunto bastante amplio de tipos penales, que también afectan a otros bienes jurídicos, como la integridad de los sistemas informáticos.

Entre estos delitos se encuentran el acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, la Interceptación de datos informáticos, el daño Informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para capturar datos personales, el hurto por medios informáticos y semejantes y la transferencia no consentida de activos.

En el Título VIII se contemplan los Delitos contra los Derechos de Autor, en los cuales existen tres figuras típicas Violación a los derechos morales de autor, la Defraudación a los derechos patrimoniales de autor y la Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

Finalmente, dentro del Título XII se contemplan los Delitos contra la seguridad pública y los delitos de peligro común o que pueden ocasionar grave perjuicio para la comunidad y otras infracciones, en el cual se contempla el delito de daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Dentro de la Comunidad Andina, y también de la región Sudamérica, la legislación colombiana resulta ser una de las pioneras en incorporar la figura del perito informático para la investigación del delito, siendo así que dentro del Código de Procedimiento Penal colombiano se disponen los requisitos que se requieren para poder ser perito informático, y así el artículo 408 prescribe que:

> "Artículo 408. Quiénes pueden ser peritos. Podrán ser peritos, los siguientes: 1. Las personas con título legalmente reconocido en la respectiva ciencia, técnica o arte. 2. En circunstancias diferentes, podrán ser nombradas las personas de reconocido entendimiento en la respectiva ciencia, técnica, arte, oficio o afición, aunque se carezca de título. A los efectos de la cualificación podrán utilizarse todos los medios de prueba admisibles, incluido el propio testimonio del declarante que se presenta como perito".

En la normativa colombiana se disponen menos requisitos para poder desempeñar las actividades de perito, pues en primer lugar se establece la necesidad de que el perito sea un experto dentro de un área de estudio, pero no se le impone un tiempo en el cual haya realizado

este tipo de actividades, sino solamente la obligación de que tenga experticia dentro de un área del saber humano.

La norma también permite que el conocimiento que haya adquirido el perito en el área de trabajo, no sea únicamente académico, sino que también podrá realizar la pericia quien posea los conocimientos empíricos lo suficientemente altos para desarrollar la actividad encomendada. Tampoco se estipula un tiempo mínimo en el cual el perito deba haber realizado sus actividades.

El mismo Código de Procedimiento Penal colombiano también dispone dentro de artículo seguido, cuales son las personas que están prohibidas de realizar actividades periciales, siendo estas:

> "Artículo 409. Quiénes no pueden ser nombrados. No pueden ser nombrados, en ningún caso: 1. Los menores de dieciocho (18) años, los interdictos y los enfermos mentales. 2. Quienes hayan sido suspendidos en el ejercicio de la respectiva ciencia, técnica o arte, mientras dure la suspensión. 3. Los que hayan sido condenados por algún delito, a menos que se encuentren rehabilitados".

Respecto de las prohibiciones por la cuales una persona no puede ser un perito informático, la misma prescribe en primer lugar la minoría de edad, aquellos que estén sujetos a una interdicción y también aquellos que tengan alguna discapacidad. Se prohíbe a quienes hayan sido suspendidos de manera temporal o definitiva comparecer como peritos en juicios posteriores y finamente, aquellos que esté cumpliendo una condena por un delito y que no haya sido rehabilitados hasta el momento del nombramiento de la pericia.

6.2.4 Legislación peruana

La Constitución de Perú, al igual que los demás países del área andina, constituye el instrumento supremo sobre el cual se estructura el Estado donde se exponen las directrices de la administración estatal, lo que incluye todo lo relacionado con la administración de justicia. Precisamente, es dentro de los principios de la administración de justicia dispuestos en el artículo 139, numeral 3, de la Carta Política, en donde se consagra el derecho al debido proceso que asiste a todas las personas en un proceso judicial

> "3. La observancia del debido proceso y la tutela jurisdiccional. Ninguna persona puede ser desviada de la jurisdicción predeterminada por la ley, ni sometida a procedimiento distinto de los previamente establecidos, ni juzgada por órganos jurisdiccionales de excepción ni por comisiones especiales creadas al efecto, cualquiera sea su denominación."

En lo que se refiere a los principios sobre los cuales se debe desarrollar la actividad probatoria, la Constitución peruana no hace ninguna referencia, tampoco a la actividad pericial como tal,

sino que únicamente consagra al debido proceso, que si bien es cierto tiene cierto contenido dentro de la misma normativa peruana, también incluye los aspectos que se han desarrollados en los instrumentos internacionales ratificados por el Estado peruano, en los cuales si se establece la necesidad de que la prueba sea realizada de manera adecuada y sin violación de ley.

Una diferencia sustancial que existe en cuanto a la regulación de los delitos informáticos dentro de la legislación peruana, es que los mismos se encuentran tipificados en una normativa independiente del Código Penal, de allí que es mucho más fácil identificarlos dentro de esta normativa, que tan solo tiene 13 artículos.

En el primer artículo de esta norma, se dispone cuál es su objeto y finalidad, siendo la siguiente:

> "Prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia."

Dentro del segundo capítulo de esta ley se disponen los delitos que producen daño informático, empezando por tipificarse el acceso ilícito a los sistemas informáticos, atentado a la integridad de datos informáticos y finalmente el atentado a la integridad de sistemas informáticos, siendo que en los primeros se protege la información que guardan los mismos, mientras que en el segundo se protege la integridad del sistema como tal, ya que muchas veces son los sistemas públicos los que sufren el ataque de algún delito.

En el tercer capítulo, se dispone los delitos informáticos contra la indemnidad y libertad sexuales, siendo en este caso una sola figura penal la prevista para tutelar los derechos de los menores de edad, siendo este las proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, conocido como *grooming.*

En el capítulo cuarto de esta norma se prescriben los delitos informáticos contra la intimidad y el secreto de la comunicación, que igualmente, consta de una sola figura típica para sancionar a os infractores, siendo esta la Interceptación de datos informáticos, siempre que la misma hay sido deliberada.

El quinto capítulo de la norma contempla los delitos informáticos contra el patrimonio, en el cual se tutela una sola clase de tipo penal, que se trata del fraude informático, que solo cuenta con una figura penal y con un conjunto como se ha señalado desde la doctrina. Un capítulo más adelante, se tipifica el delito de suplantación de identidad, cuando la misma se ha

realizado por medios electrónicos. El último de los delitos informáticos, es el abuso de mecanismos y dispositivos informáticos

Si bien es cierto, la gran mayoría de delitos informáticos se encuentra tipificada dentro de esta ley, dentro del Código Penal peruano también existen otro conjunto de figuras que constituyen estos delitos informáticos, y que requieren se mencionados, en razón de los bienes jurídicos tan importantes que tutelan.

En el Titulo IV, que se refiere a los delitos de libertad, se encuentran varias figuras típicas, siendo estas la explotación sexual comercial infantil y adolescente en ámbito del turismo; la publicación en los medios de comunicación sobre delitos de libertad sexual a menores; y, la pornografía infantil y las proposiciones sexuales a niños, niñas y adolescentes.

Dentro del artículo 196 A del Título V se dispone también de un delito en contra del patrimonio; mientras que en el Titulo VI se disponen los delitos en contra de los derechos intelectuales, dentro de esta categoría se encuentran la Reproducción, difusión, distribución y circulación de la obra sin la autorización del autor, el plagio, la elusión de medida tecnológica efectiva y los productos y servicios destinados a esta misma elusión y finalmente los delitos contra la información sobre gestión de derechos.

En cuanto a los delitos contra el patrimonio están en el Título V y son el hurto utilizando el espectro radioeléctrico para la transmisión de señales de telecomunicación ilegales y la utilización de los dispositivos para asistir a la decodificación de señales de satélite portadoras de programas.

En lo que se refiere a los requisitos para ser perito informático, la legislación peruana, dentro del Código de Procedimientos Penales, no detalla mayor disposición, sino que únicamente prescribe dentro de su artículo 160 que: “Artículo 160.- El juez instructor nombrará peritos, cuando en la instrucción sea necesario conocer y apreciar algún hecho importante que requiera conocimientos especiales. Este nombramiento se comunicará al inculpado, al Ministerio Público y a la parte civil”.

En cuanto a los requisitos para ser perito, los mismos se contemplan de manera general y no específicamente para el caso informático, dentro del Reglamento del Registro de Peritos Fiscales, dispone dentro de su artículo 13 que los mismos deberán ser profesionales dentro de un área específica, y que deberán contar con el tiempo de cinco años de experiencia en la misma.

Según esta misma norma, los peritos deberán tener titulación profesional o de especialista en el área que soliciten se les acredite como peritos, la colegiatura en el organismo que les

acredite para actuar como peritos o dentro del área criminológica, pero además deberán estar en goce de los derechos civiles y no contar con antecedentes penales.

De las normativas analizadas hasta el momento de los países miembros de la CAN, es dentro de la legislación peruana en donde se observa que existen requisitos que son más estrictos para poder ser un perito, ya que se requiere de al menos una doble capacitación, no solo en el área en el cual se va a realizar el peritaje, sino que además se exige una colegiatura en materia de pericia, al igual que lo contempla la legislación española.

6.2.5 Legislación boliviana

La Constitución de la República de Bolivia, es la norma suprema que prevalece por encima de cualquier otra norma del ordenamiento jurídico, de acuerdo con lo previsto dentro del artículo 410 de la misma Constitución:

> "La Constitución es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario, ratificados por el país."

De esta manera, la Constitución reconoce expresamente el orden aplicación de las normas jurídicas bajo la concepción clásica de la pirámide Kelsen, de modo que los derechos previstos en la Constitución y en los instrumentos internacionales de derechos humanos prevalecen por encima de las demás normas, debiéndose respetar los derechos de protección de las personas, como el debido proceso, previsto dentro del artículo 115 que prescribe:

> "Artículo 115.I. Toda persona será protegida oportuna y efectivamente por los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos. II. El Estado garantiza el derecho al debido proceso, a la defensa y a una justicia plural, pronta, oportuna, gratuita, transparente y sin dilaciones".

En la norma suprema boliviana se contempla el derecho al debido proceso, el mismo que se configura en todos los procedimientos en los cuales se esté resolviendo acerca de los derechos de las personas, siendo una obligación gubernamental que se la justicia sea efectiva y expedita y que garantice el derecho a la defensa de las personas.

En lo que se refiere al aspecto probatorio, el principio de legalidad de la prueba se halla previsto en la misma Constitución, pero de manera independiente del debido proceso, concretamente dentro del artículo 25, numeral 4 en el que se prevé que "La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal".

En lo que se refiere a los delitos informáticos en la legislación boliviana, se encuentran tipificados dentro de tres normas, la primera de éstas es el Código Penal, aunque no están dispuestos dentro de un solo capítulo, sino que se ubican de acuerdo con el bien jurídico al que afectan.

Es así que, en primer lugar, están los delitos informáticos de contenido, pues en el artículo 281 *cuater*, se halla tipificado el Pornografía y espectáculos obscenos con niños, niñas o adolescentes. Asimismo, dentro de los artículos 214 y 215 se disponen los delitos de daño informático, los cuales contemplan dos figuras, la primera es el atentado contra la seguridad de los servicios públicos y la segunda sanciona a este mismo atentado, pero cuando se afecte a bienes de gran valor científico, artístico, militar o económico, en cuyo caso se aplicará una pena mayoritaria.

Dentro de los artículos 300 y 301 se contemplan los delitos en contra de la seguridad de los datos, siendo estos los de violación de la correspondencia y papeles privados y la Violación de secretos en correspondencia no destinada a la publicidad, siempre que las mismas se realicen por medios informáticos.

Otros de los delitos que se contemplan dentro la normativa penal, y que también se relacionan con el contenido, y que afectan a la integridad sexual de los menores de edad son los previstos entre los artículos 318 y 321, entre los que se encuentran la corrupción de menores, corrupción de mayores, la corrupción agravada y el proxenetismo.

Así también, dentro de los artículos 323 bis y 324 se contemplan otros tipos penales que afectan a los referidos bienes jurídicos, siendo estos lo de pornografía de niñas, niños o adolescentes y de personas jurídicamente incapaces y Publicaciones y espectáculos obscenos.

Finalmente, dentro de la normativa penal se contemplan los delitos de manipulación informática y alteración, acceso y uso indebido de datos informáticos, mismo que afectan la integridad de los datos públicos, y que dentro de la clasificación de este tipo de delitos se ubican en la categoría de fraudes electrónicos.

En cuanto a la designación de los peritos que actúen en los procedimientos penales y los requisitos que deben cumplir, dentro del artículo 205 del Código de Procedimiento Penal se dispone:

> "Artículo 205º. (Peritos). Serán designados peritos quienes, según reglamentación estatal, acrediten idoneidad en la materia. Si la ciencia, técnica o arte no está reglamentada o si no es posible contar con un perito en el lugar del proceso, se designará a una persona de idoneidad manifiesta".

Conforme a lo previsto dentro de esta norma, se observa que para que las personas puedan ser designadas como un perito de la causa, las mismas deberán haber cumplido con los requisitos reglamentarios dispuestos en la normativa respectiva, pero además deberán tener una amplia capacitación dentro del área a la cual se refiere el proceso en cuestión.

En cuanto a los requisitos para desempeñarse como perito, los mismos se hallan previstos dentro del Reglamento del registro y actuación de peritos, intérpretes y traductores, promulgado por el Tribula Supremo de Justicia, en el que se dispone que los peritos, no deberá poseer Antecedentes Penales ni expedientes disciplinarios en el ámbito profesional, para lo cual, el Colegio al que pertenecen deberá entregarles un certificado.

En cuanto a los requisitos de carácter académico, se deberá tener "Título en Provisión Nacional, o certificación similar que acredite el área de conocimiento adquirido; Títulos de cursos de post grado (Diplomado, Maestría, Doctorado). Asistencia a cursos de actualización sobre la especialidad adquirida"; mientras que en lo relativo a la experiencia profesional que se debe acreditar, se exige que sea mínima de un año en la rama en la cual el perito se desempeñará.

Además de esta experiencia académica y profesional que se debe acreditar, se requiere que el perito haya asistido a los cursos de capacitación que realiza la Escuela de Jueces del Estado de acuerdo con cada una de las especialidades y también aspectos legales.

Una vez que se ha realizado el correspondiente análisis de la legislación boliviana, es pertinente señalar que estos son los países que conforman la CAN, de manera que se pueden apuntar algunas conclusiones acerca de lo analizado hasta el momento. Es así que en primer lugar se observa que la mayor parte de países tienen una legislación constitucional que protege el debido proceso como un derecho fundamental a ser respetado en los procedimientos penales, lo que implica que se debe respetar todas las garantías de este derecho, lo que significa el respeto al principio de legalidad de la prueba.

También se ha podido evidenciar que, se cuenta con un marco adecuado en la tipificación de los delitos informáticos, por lo que se protegen a los distintos bienes jurídicos a los que afecta el cometimiento de estos ilícitos, de manera que existe una relación entre los delitos tipificados en cada uno de los países.

Sin embargo, un aspecto en el cual se ha notado serias deficiencias tiene que ver con la designación de los peritos y los requisitos que se deben cumplir, ya que en ningún caso existe una normativa especializada que trae acerca del perito informático, sino que en los distintos países existe solo un Reglamento que establece condiciones generales para ser perito en cualquier área, pero no se centra en el perito informático como tal. También se observa

deficiencias en la capacitación, pues dentro de la legislación española es requisito indispensable que, además de acreditar la formación académica en el área científica, se acrediten estudios en centros de formación de peritos o en ciencias criminológicas, requisito que se omite en los países de la CAN.

6.2.6 Legislación argentina

En la legislación argentina, la Constitución de la Nación Argentina constituye la norma suprema, y en la misma se ha dispuesto, algunos derechos que están relacionados con la protección del derecho al debido proceso, aunque dentro de esta legislación no se le otorga ese nombre.

Es así que dentro del artículo 8 de esta norma, se disponen las garantías judiciales, que deberán ser aplicadas cuando se investiguen los delitos, y dentro del numeral 2 se prescribe que:

> "2. Toda persona inculpada de delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad. Durante el proceso, toda persona tiene derecho, en plena igualdad, a las siguientes garantías mínimas (…) f) derecho de la defensa de interrogar a los testigos presentes en el tribunal y de obtener la comparecencia, como testigos o peritos, de otras personas que puedan arrojar luz sobre los hechos".

En la normativa constitucional argentina se disponen un conjunto de garantías mínimas que se deberán garantizar al momento de la investigación de un hecho ilícito, que se relacionan con la presunción de inocencia, la igualdad de condiciones, pero sobre todo la posibilidad de ejercer el derecho a la defensa en todas sus formas, lo que incluye el interrogar a los peritos que actúen en el caso.

En lo que se refiere a la investigación de los delitos informáticos, los mismos constan dentro de tres normas, el Código Penal, la ley de actos discriminatorios y el Régimen legal de la Propiedad Intelectual. En la primera norma, dentro del artículo 128 se dispone el primer delito de contenido, que es la pornografía infantil en sus distintas formas, tanto el almacenamiento, como la venta de este material está absolutamente prohibido.

En el artículo 131 se dispone el delito de contacto por medios electrónicos de una persona mayor de edad con una menor, para fines sexuales, conocido también como *grooming*

En los artículos 153 y 153 bis se dispone los delitos que afectan a la integridad de la base de datos, empezando por el acceso a la base de datos protegida sin la autorización del legítimo propietario de la misma, sin importar cual haya sido la finalidad para el cometimiento de este

delito y en el artículo 155 la relevación de secretos informáticos. Estos mismos delitos se encuentran tipificados dentro

Por otra parte, en el artículo 73 se disponen las distintas formas de delitos de fraude electrónico. En cambio, dentro del artículo 183 se prescribe el delito de daño informático, ya sean datos, programas o sistemas informáticos. Finalmente se tipifica el delito de interrupción de comunicaciones telefónicas o de cualquier otra forma.

Por su parte, la Ley 23.592 de Actos Discriminatorios, dispone un único delito informático, siendo este la difusión de actos se discriminación basados en idas de superioridad por cualquier motivo, religioso, étnico u otros, siempre que el mismo se realice por medios digitales.

Finalmente, se disponen dentro de la Ley 11.723 de Régimen Legal de la Propiedad Intelectual los actos que defrauden los derechos de propiedad intelectual, es decir, la apropiación indebida de esto derechos o su uso sin el respectivo consentimiento de los autores legítimos.

En lo que se refiere a los requisitos para poder sea designado como perito, dentro del Código Procesal Penal Federal en su artículo 68 se prescribe:

> "Artículo 168.- Calidad habilitante. Los peritos deberán tener título habilitante en la materia relativa al punto sobre el que dictaminarán, siempre que la ciencia, arte o técnica esté reglamentada. En caso contrario deberá designarse a una persona de idoneidad manifiesta. No podrán desempeñarse como peritos las personas a quien la ley reconociere la facultad de abstenerse de prestar declaración testimonial. No regirán las reglas de la prueba pericial para quien declare sobre hechos o circunstancias que conoció espontáneamente, aunque utilice para informar las aptitudes especiales que posee en una ciencia, arte o técnica. En este caso regirán las reglas de la prueba testimonial".

Conforme a lo previsto dentro de esta norma se evidencia que se requiere de la calidad habilitante para poder realizar cualquier pericia dentro del sistema judicial, para lo cual deberán tener cualquier título habilitante dentro de la materia en la cual van a desarrollar la pericia, y deberán haber sido registrados en cada una de las asociaciones de peritos que se encuentran a nivel nacional, considerando la estructura federal que mantiene este Estado.

En cuanto a los requisitos que se necesitan para poder ser inscritos, en primer lugar se requiere del certificado de antecedentes penales expedido por la Policía Nacional, así también como la acreditación académica de haber sido formado dentro de las áreas en las cuales se busca ser perito, pero además se deberá acreditar la "Constancia de haber realizado y aprobado actividades de capacitación y/ o actualización forense, científica, artística o profesional para Peritos Judiciales dictados por Universidades o instituciones académicas

públicas o privadas, Consejos o Colegios profesionales", conforme se dispone en el Reglamento de inscripción de peritos judiciales del Poder Judicial.

Dentro de la normativa argentina, se observa cómo se requiere una doble acreditación para realizar la actividad pericial, ya que por una parte se requieren de los conocimientos científicos dentro del área a realizar la pericia, y por el otro, haber tenido alguna formación o capacitación como perito, aunque tampoco se señala de manera específica cual será la formación del perito informático, sino que los mismos se dan de manera general para los profesionales de todas las áreas.

6.2.7 Legislación mexicana

La Constitución Política de los Estados Unidos Mexicanos, es el máximo instrumento jurídico de México, y dentro del mismo se contemplan los derechos más importantes que se garantizan a todas las personas, entre las que se encuentra el debido proceso, y concretamente dentro del artículo 20 se prescriben algunos principios que deberá cumplir se manera obligatoria en los procesos penales, y así se prescribe que:

> "Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación. A. De los principios generales: (…) IX. Cualquier prueba obtenida con violación de derechos fundamentales será nula (…)".

La normativa constitucional es clara al establecer que, para garantizar con el cumplimiento del debido proceso, se deberá cumplir con las garantías constitucionales mínimas, entre las que están el principio de exclusión de la prueba ilegal de allí que la actividad del perito deba realizarse dentro del apego de las normas constitucionales y legales.

En cuanto a los delitos informáticos, los mismos se hallan previstos dentro de dos normas, siendo el Código Penal Federal y la Ley Federal del Derecho de Autor. Dentro del primero, se encuentran los artículos 211 y 211bis, en los que se tipifican los delitos de Revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Asimismo, en cuanto a los delitos de contenido, dentro de los artículos 202, 202 bis y 203 se tipifican los delitos de Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo.

Lo delitos de ataques a las vías de comunicación y violación de correspondencia, que se realizan a través de medios digitales, se encuentran tipificados dentro de los artículos 167,

168 y 168 bis. Finalmente, dentro de los artículo 424 al 429 se encuentran tipificados los Delitos en Materia de Derechos de Autor.

En lo que se refiere a la Ley Federal del Derecho de Autor, la norma solo dispone una prohibición expresa de importar, fabricar o vender aparatos o prestar servicios destinados a eliminar de las protecciones que tiene los programas de cómputo o demás elementos electrónicos.

Ya en lo que se refiere de manera concreta a los requisitos que se requieren para ser peritos, el Código de Nacional de Procedimientos Penales prescribe una disposición general dentro de su artículo 369:

> "Artículo 369. Título oficial Los peritos deberán poseer título oficial en la materia relativa al punto sobre el cual dictaminarán y no tener impedimentos para el ejercicio profesional, siempre que la ciencia, el arte, la técnica o el oficio sobre la que verse la pericia en cuestión esté reglamentada; en caso contrario, deberá designarse a una persona de idoneidad manifiesta y que preferentemente pertenezca a un gremio o agrupación relativa a la actividad sobre la que verse la pericia".

De acuerdo con lo previsto dentro de esta norma, se puede comprender como la persona que quiere actuar como perito requiere no encontrarse en alguna de las prohibiciones para ejercer su actividad, entre las que se encuentran el no tener antecedentes penales, ni estar sancionado administrativamente por el Estado o por el colegio al que pertenece por faltas disciplinarias o en mora de pagos por concepto de pensiones alimenticias u obligaciones con el Estado.

Habiendo cumplido con este primer grupo de requisitos, el perito deberá además cumplir con las relacionadas a la acreditación académica y de experiencia, para lo cual deberá tener un título habilitante dentro de la rama científica sobre la cual prestará sus servicios, y en lo que se refiere a la experiencia, no se determinan un número de años mínimos que se requieran para realizar la actividad pericial.

Siendo México un Estado federado, existe más de un instrumento de regulación para la habilitación de peritos en las distintas áreas, por lo que cada Estado cuneta con un Reglamento para la inscripción y habilitación de peritos judiciales, lo que incluye también el ámbito informático.

Por esta razón, no se puede señalar un solo conjunto de requisitos para los peritos informáticos en este país, pero con base a algunos instrumentos analizados, se puede señalar que los requisitos estándar son tener un Título Profesional expedido por Institución autorizada, documentos de identidad actualizados, residencia dentro del Estado a ejercer la pericia, tener prestigio profesional, no tener antecedentes penales, tener capacitaciones como peritos o

cursos del Consejo de la Judicatura del país, tener más de tres años en la profesión en la cual se ejercerá la pericia.

En este punto, debe señalarse que existen algunos reglamentos (como el del Estado Querétaro o Nayarit) en los cuales, se realiza una clasificación más técnica de los peritos, de acuerdo con las áreas en las cuales llevaran a cabo su labor de investigación en el ámbito penal, diferenciando algunos de los requisitos de acuerdo con estos criterios de división.

De manera que puede verse que la legislación de este país norteamericano, presenta un mayor avance en cuanto a la actividad pericial que en los países sudamericanos, sobre todo en lo que se refiere al criterio de selección de los peritos y de los requisitos que tienen una mayor exigencia al momento de seleccionar al persona pericial, solicitando no solo una formación como profesionales en la distintas áreas, sino que además se busca que exista una formación criminológica o pericial, dentro de las distintas capacitaciones que se realizan incluiste pro parte de organismos estatales.

6.2.8 Legislación estadounidense

En lo que se refiere a la legislación en contra de los delitos informáticos, una de las legislaciones más importantes y desarrolladas es la estadounidense, ya que tiene una gran experiencia en temas de seguridad informática, así como organismos especializados dedicados a la lucha contra los ataques informáticos.

Sin embargo, la Constitución de Estados Unidos, garantiza también los derechos más importantes a quienes están siendo investigados por un delito informático o cualquier otro delito, permitiendo la realización de las investigaciones de delitos informáticos a peritos expertos en este campo. Es así que, dentro de la Enmienda V, se garantiza en primer lugar el derecho al debido proceso o tutela efectiva de la siguiente manera:

> "Nadie estará obligado a responder de un delito castigado con la pena capital o con otra infamante si un gran jurado no lo denuncia o acusa, a excepción de los casos que se presenten en las fuerzas de mar o tierra o en la milicia nacional cuando se encuentre en servicio efectivo en tiempo de guerra o peligro público; tampoco se pondrá a persona alguna dos veces en peligro de perder la vida o algún miembro con motivo del mismo delito; ni se le compelerá a declarar contra sí misma en ningún juicio criminal; ni se le privará de la vida, la libertad o la propiedad sin el debido proceso legal; ni se ocupará la propiedad privada para uso público sin una justa indemnización".

Conforme se dispone dentro de la Constitución norteamericana, todos los seres humanos tienen el derecho a un juicio justo, en el cual se garantice un conjunto mínimo de derechos de protección, ya que para ponerse en peligro un derecho de una persona, cualquiera que fuera,

debe producirse un proceso judicial, que respete los derechos de los procesados, incluyendo el derecho a la defensa

Ya en lo que se refiere a los delitos informáticos, debe señalarse que se trata de una de las legislaciones que más tipos penales informáticos tiene, y además los mismos se cometen en distintos grados, formas y modalidades; por ejemplo, un tipo penal de fraude electrónico puede contener hasta 20 subtipos de delitos que se relacionan con el principal; y esto sucede en cada uno de los delitos que se encuentran tipificados dentro del "USC *Crimes and Criminal Procedure*", traducido como USC Delitos y Procedimiento Penal".

Precisamente dentro del Título 18 que se refiere a los delitos y procedimiento penal, se encuentra tipificadas un conjunto de distintas acciones, siendo el primer grupo los delitos de fraude, entre los que se encuentran el artículo 1029 referente al fraude y actividades relacionadas en relación con los dispositivos de acceso, el artículo 1030 que tipifica el delito de fraude y actividades relacionadas en conexión con computadoras y el artículo 1037 relativo al fraude y actividades relacionadas en relación con el correo electrónico y también dentro del artículo 1028 el fraude y actividades relacionadas en relación con documentos de identificación, características de autenticación e información.

Como se observa, a diferencia de los delitos tipificados en otras legislaciones, en la legislación norteamericana se distinguen cuatro grandes grupos de delitos de fraude electrónico, y como ya se ha señalado, muchos de estos contienen una cantidad muy amplia de delitos derivados de los primeros, siendo una de las legislaciones más severas en cuanto a las conductas sancionables y las penas que se aplicarán.

Así también, dentro del artículo 1028 A, se tipifica el delito de Robo de identidad agravado, que sanciona a las personas que atenten contra el derecho a la identidad de las personas, y la utilicen para beneficio personal en cualquier norma, utilizando para ello distintos medios electrónicos.

En lo que se refiere a los delitos de contenido, la legislación estadounidense los contempla dentro de dos cuerpos legales, un conjunto menor se encuentra dispuesto dentro del mismo USC Delitos y Procedimiento Penal, mientras que otro está tipificado dentro del Código de Delitos y correcciones de Guam.

En cuanto a los que se encuentran dentro del primer grupo, el artículo 2251 tipifica los delitos de explotación sexual de niños, mientras que el 2252 se refiere a ciertas actividades relacionadas con material relacionado con la explotación sexual de menores y el 2252 A, se refiere a ciertas actividades relacionadas con material que constituye o contiene pornografía infantil.

Dentro del siguiente grupo de delitos se contemplan aquellas infracciones que se encasillan también dentro de los fraudes electrónicos, como el artículo 2252B que se refiere a los nombres de dominio engañosos en Internet; el artículo 2252C que se refiere a las palabras o imágenes digitales engañosas en Internet. Los artículos 2253 y 2254 se refiere al decomiso civil y penal, mientras que en los artículos 2257 y 2257 A se refieren a los requisitos de mantenimiento de registros y a los requisitos de mantenimiento de registros para conducta sexual simulada. Finalmente, dentro del artículo 2261A se encuentra el delito de acecho, que se lo puede identificar con las conductas del ciberacoso.

Dentro del tercer grupo de delitos se encuentran los delitos en contra de la propiedad intelectual, empezando en el artículo 2319 en el cual se tipifica la infracción penal de un derecho de autor y en el artículo 2319A se encuentra la Fijación no autorizada y tráfico de grabaciones de sonido y videos musicales de actuaciones musicales en vivo. En el artículo 2319B se encuentran dispuesto el delito de grabación no autorizada de películas en una instalación de exhibición de películas.

En el artículo 2320 se tipifica el tráfico de bienes o servicios falsificados, mientras que en el artículo 2701 se encuentra el acceso ilegal a comunicaciones almacenadas. En los artículos 2702, 2703 y 2704 se refieren a las infracciones por divulgación de las comunicaciones o registros de clientes y su respaldo. Finalmente, entre los artículos 3121 y 3125 se encuentran los delitos de prohibición del uso de dispositivos de registro de rastreo.

En cuanto al segundo cuerpo legal que tipifica los delitos informáticos, están contemplados dentro de los delitos y correcciones de Guam, y tipifican principalmente delitos en contra de la integridad sexual de los menores, empezando por la eexhibición electrónica indecente a un niño, posteriormente están las infracciones de atracción electrónica de un niño como delito grave en distintos grados y la posesión y difusión de pornografía infantil. Finalmente se tipifica la divulgación de incumplimiento de seguridad de información personal computarizada por un individuo o entidad.

El último cuerpo legal que contiene delitos en contra de la seguridad informática es el USC: Título 17 - Derechos de autor, en el cual se contemplan las infracciones por Elusión de los sistemas de protección de derechos de autor y las infracciones penales para fines de ventaja comercial o ganancia financiera privada mediante la reproducción o distribución, incluso por medios electrónicos, obras con derechos de autor.

En lo que se refiere a la designación de los peritos y de los requisitos que deben cumplir para poder cumplir con esta finalidad, los mismos se hallan previstos tanto dentro de la normativa como de los preceptos jurisprudenciales, difiriendo en diversos aspectos con el derecho

Latinoamérica, pues al tratarse de un sistema de derecho anglosajón del *common law*, las características del proceso penal difieren en diversos aspectos, lo que también se refleja en la actividad de los peritos.

La actividad de los peritos se encuentra regulada por la R*ule 702. Testimony by Expert Witnesses,* que traducida significa Regla 702. Testimonio de testigos expertos, en la cual, no solamente se disponen requisitos para que las personas puedan actuar como peritos, sino que también se estipulan reglas para que su testimonio pueda ser admisible dentro del procedimiento penal. Esta regla en concreto determina que:

> "Un testigo que esté calificado como experto por conocimiento, habilidad, experiencia, capacitación o educación puede testificar en forma de opinión o de otra manera si: (a) el conocimiento científico, técnico u otro conocimiento especializado del experto ayudará al evaluador de hechos a comprender la evidencia o determinar un hecho en cuestión; (b) el testimonio se basa en hechos o datos suficientes; (c) el testimonio es producto de principios y métodos confiables; y (d) el experto ha aplicado de manera confiable los principios y métodos a los hechos del caso."

En el sistema norteamericano, no es suficiente que el perito cumpla una serie de requisitos para poder declarar como un testigo experto, principalmente en cuanto a su capacitación académica o como criminólogo y el tiempo que se ha dedicado a ejercer su actividad como profesional, sino que además se deberá demostrar que su participación dentro del procedimiento penal se encuentra plenamente justificada.

Este sistema tiene lógica en el sistema estadounidense, debido a que en un inicio los testigos expertos o peritos, eran llevados por cada una de las partes, por lo que resultaban poco objetivos al momento de aportar con su conocimiento para la resolución de la causa, por lo que a través de los fallos pronunciados en los casos Daubert v. Merrell Dow Pharmaceuticals, se introdujeron cambios para valorar los requisitos y el aporte que un perito puede realizar dentro de un proceso penal (Aguirrezabal, 2012).

6.2.9 Legislación francesa

Dentro de la legislación francesa, cuyo carácter es eminentemente política, no se disponen ninguna norma relacionada con la protección de los derechos en el ámbito judicial, ni siquiera en lo relaciona al debido proceso, por lo que es necesario analizar cuáles son los delitos informáticos que se han tipificado dentro de esta legislación.

El código penal francés, tipifica una serie de delitos dentro de la legislación francesa, entre los que se encuentran en primer lugar, los delitos que vulneren la privacidad de las personas por medios electrónicos, mismos que se hallan dispuestos en el artículo 226-1; mientras que

dentro del artículo 226-3 se sanciona a aquellas personas que hayan fabricado, almacenado o vendido aparatos tecnológicos a través de los cuales se pudieren cometer delitos informáticos.

Dentro de este mismo grupo de delitos, se sancionan en los artículos 226-18 la recopilación de datos personales por cualquier medio que fuera fraudulento, deshonesto o ilegal; mientras que en el artículo 226-18-1 se sanciona el procesamiento de datos personales de las personas naturales.

Dentro de los artículos 226-21 y 226-22 se sanciona el registro, archivo o trasmisión de información personal, si la autorización de la persona titular, y también cunado la misma haya sido divulgada hacia otras personas igualmente sin consentimiento expreso del titular. Cabe señalar que, en todos estos casos, además de la responsabilidad de la persona natural que ha cometido la actuación, también se ha previsto la existencia de responsabilidad para la persona jurídica, de conformidad con los protocolos internacionales que buscan una lucha contra el crimen organizado.

Seguidamente, dentro del artículo 227-23, se tipifican los delitos de contenido, que en este caso se consagra en solo tipo penal, que es de pornografía infantil, ya sea que la misma se haya almacenado, grabado, trasmitido o vendido por los medios tecnológicos. En este caso también se sanciona cuando se haya utilizado a una persona mayor de edad, cuya apariencia física pueda ser confundida con la de un menor de edad.

Asimismo, dentro de este mismo grupo de delitos, en el artículo 227-24, se tipifica y castiga a las acciones que se trasmita de manera masiva por los medios tecnológicos, mensajes de carácter extremadamente violentos, los que fomenten los actos terroristas, con contenido pornográfico o que promuevan la denigración de la dignidad humana.

En los artículos 226-16, 226-16-1 y 226-17 se tipifica los delitos en los cuales se haya realizado un procesamiento de datos personales en los cuales no se haya protegido la información adecuadamente, de modo que los mismos por un manejo negligente pudieren haber sido perdidos o afectados en distinta forma.

En el siguiente grupo de normas se contemplan los delitos que hayan producido daño informático, sancionándose dentro del artículo 323-1 el acceso no autorizado a un sistema informático, mientras que en el artículo 323-2 se sanciona el obstaculizar el acceso a los sistemas informáticos. En el artículo 323-3 la extracción, reproducción, transmisión, alteración o eliminación de sistemas de procesamiento de datos de manera fraudulenta.

En el artículo 441-1 y Artículo 441-2 se tipifica las distintas formas de fraudes electrónicos, determinándose para tales efectos que:

> "Una falsificación es cualquier alteración fraudulenta de la verdad, de tal naturaleza que pueda causar daño y realizada por cualquier medio, por escrito u otro medio de expresión de pensamiento que tenga el propósito o que pueda tener el efecto de establecer prueba de un derecho o hecho con consecuencias legales".

En el artículo 411-9 se sanciona la destrucción de documentos, materiales, equipos, dispositivos técnicos o sistemas automatizados que contengas información importante, más si con los mismos se ha perjudicado gravemente a la sociedad o también a la seguridad del Estado

En lo que se refiere a los delitos informáticos que afectan a la propiedad intelectual, los mismos se encuentran regulados dentro del Código de propiedad intelectual en su artículo R335-2; mientras que el Código monetario y financiero dispone en su artículo L163-3, la falsificación de cheques u otros documentos crediticios; y en el artículo L163-4 a quienes ofrezcan equipos, instrumentos o programas destinados al cometimiento de los delitos informáticos.

> "Un experto judicial es responsable de dar al juez una opinión sobre puntos técnicos específicos. Hay expertos en una amplia variedad de disciplinas (médico, especialista en construcción) Su opinión no es vinculante para los jueces, que siguen siendo libres. Un experto forense es un profesional especializado en una técnica determinada que pone su competencia al servicio de la justicia cuando la solicita. Más allá del juramento, el experto que se adhiere a una asociación se compromete a respetar las reglas de ética establecidas por las Sociedades de Expertos del Consejo Nacional de Justicia" (Forensic, 2018, pág. 8).

Como se observa, al igual que en la mayoría de las legislaciones, dentro de la francesa el perito tiene la finalidad de auxiliar al juzgador en temas que resultaren demasiado técnicos, para lo cual hará uso de los medios tecnológicos a su disposición explicando los resultados de la investigación adquirida el juzgador.

Respecto de los requisitos que se deben cumplir, para lograr la acreditación como perito en Francia, la editorial Forensic señala lo siguiente:

> "Las condiciones generales para figurar en una lista de expertos se definen en el artículo 2 del decreto de 23 de diciembre de 2004: se refieren en general al honor y la probidad del candidato, su experiencia y calificación en la especialidad reclamada, así como su necesaria independencia en el ejercicio de su actividad profesional" (Forensic, 2018, pág. 8).

Nuevamente los requisitos para ser perito dentro de esta legislación se encuentran relacionados con la acreditación de la capacidad que tiene en el ámbito académico, así como demostrar su buen honor y el tiempo por el cual está ejerciendo la profesión con la debida diligencia.

6.2.10 Legislación internacional

A nivel mundial existen algunos entes reguladores que están aportando con información actualizada, para tipificar o categorizar las conductas delictivas de los delincuentes, sin duda día a día se vuelven más diversas y complejas. Estas entidades son:

- Organización de las Naciones Unidas (ONU)
- Organización de Cooperación y Desarrollo Económico (OCDE)
- Unión Internacional de Telecomunicaciones(UIT)
- Policía Europea EUROPOL
- Organización Internacional de Policía Criminal (INTERPOL)

Esta última organización es la más importante, puesto que cuenta con 194 países miembros, cuyo objetivo es cooperar con la policía de estos países para combatir la delincuencia internacional y conseguir un mundo más seguro.

Desde el punto de vista del derecho internacional, se puede afirmar que no existe un tratado internacional que regule toda la actividad de los delincuentes informáticos y se los sancione de manera adecuada, aplicando un principio de territorialidad; sin embrago, con el paso del tiempo se han ido dando importantes avances en materia de protección internacional en contra de los delitos informáticos, existiendo actualmente un conjunto de instrumentos internacionales que permiten la adhesión libre que permita una mayor cooperación internacional para combatir a los delincuentes informáticos.

Precisamente, respecto de los importantes instrumentos internacionales que aseguran la protección frente a los delitos informáticos, así como la cooperación entre los distintos países miembros, la UNODC apunta el siguiente criterio:

> "Se podrían identificar cinco posibles 'grupos' de instrumentos –(i) instrumentos desarrollados en el contexto, o inspirados por el Consejo de Europa o la Unión Europea, (ii) instrumentos desarrollados en el contexto de la Comunidad de Estados Independientes o la Organización de Cooperación de Shanghái, (iii) instrumentos desarrollados en el contexto africano, (iv) instrumentos desarrollados por la Liga de los Estados Árabes, e (v) instrumentos desarrollados bajo los auspicios, o asociados con las Naciones Unidas" (Organización de Naciones Unidas, 2013, pág. 70).

Como bien explica este organismo dentro del derecho internacional existen diferentes instrumentos de regulación en contra de los delitos informáticos, muchos de los cuales se encuentra dentro del ámbito comunitario, concretamente los publicados por la Unión Europea, y que a su vez han servido para la creación de otro tipo de instrumentos.

Debe afirmase que, debido a la importante finalidad que tiene la creación de estos instrumentos, muchos de los mismos han sido ratificados por Estados que no pertenecen a esta comunidad geográfica, pero que igualmente han buscado otorgar una protección frente a las amenazas informáticas. En este mismo sentido, la UNODC apunta el siguiente criterio:

> "A nivel mundial 82 países han firmado y/o ratificado un instrumento vinculante sobre delito cibernético.82 Algunos países son miembros de más de un instrumento. A pesar de la posibilidad de participación más allá del contexto organizacional o de la redacción original, la Ilustración 3.683 muestra que –a la fecha– ningún instrumento (aparte del OP-CRC-SC de las Naciones Unidas84) ha recibido firmas o ratificaciones/adhesiones con alcance geográfico global. El Convenio sobre Ciberdelincuencia del Consejo de Europa tiene el mayor número de firmas o ratificaciones/adhesiones (48 países), incluyendo cinco Estados no miembro del Consejo de Europa.85 Otros instrumentos tienen menor alcance geográfico –la Convención de la Liga de los Estados Árabes (18 países o territorios) – el Acuerdo de la Comunidad de Estados Independientes (10 países) y el Acuerdo de la Organización de Cooperación de Shanghái (6 países). Si es firmado o ratificado por todos los Estados miembros de la Unión Africana, el proyecto de Convención de la Unión Africana podría contar con 54 países o territorios" (Organización de Naciones Unidas, 2013, pág. 71).

Como se observa, si bien no existe un instrumento global que haya sido celebrado con la finalidad de otorgar una protección frente al delito cibernético, muchos ya han dado creado con la finalidad de permitir el ingreso a los distintos países y alcanzar así acuerdos que permitan la lucha contra estos delitos, cuya naturaleza ha estado relacionada siempre con la transnacionalidad, de modo que se permite la impunidad.

Por esta razón, es importante que todos estos instrumentos se vayan ampliado y universalizando, con el objetivo de que no se afecten los derechos de las personas, pues solo así se logrará una protección efectiva frente a los mismos, ante una amenaza que es cada vez mayor, y se va incorporando en la sociedad.

7 DESARROLLO DE LA METODOLOGÍA

7.1 Consideraciones preliminares

Para el desarrollo de una Metodología de Trabajo de Sistema Pericial Informático dentro del área Andina se deben señalar previamente algunas consideraciones que resultan de gran importancia para el éxito del sistema; pues siendo la Comunidad Andina de Naciones, un Sistema de integración subregional con normativa supranacional, deben puntualizarse en primer ciertos aspectos normativos.

La CAN tiene un sistema legal compuesto por normas de dos tipos: vinculantes y no vinculantes; entre las primeras están las Decisiones, cuya competencia para la expedición la tienen únicamente dos organismos de la CAN: La Comisión de la Comunidad Andina y el Consejo de Ministros de Relaciones Exteriores de la Comunidad Andina, según se dispuso en el Acuerdo de Cartagena, mientras que las no vinculantes son las Declaraciones, que pueden ser expedidas por todos los organismos de la CAN.

Las declaraciones, al ser vinculantes, son de obligatorio cumplimiento para todos los Estados miembros de la CAN, pues de lo contrario, se puede interponer recursos de incumplimiento ante el Tribunal de Justicia de la de la Comunidad Andina, mismo que puede tomar medidas de sanción ante el incumplimiento.

Sin embargo, las normativas de la CAN, pese a tener este carácter vinculante, se basan en un sistema de cooperación internacional, pues el objetivo de las normas de la CAN ha sido el de armonizar las legislaciones de los países miembros, y no de imponerse sobre las mismas, por lo que las Decisiones que se han promulgado en las distintas áreas, han tenido la finalidad de regular aspectos dentro de la subregión que requieran cooperación internacional, sin desconocer la normativa interna de cada país.

Por esta razón, en la mayoría de casos, no se determinan autoridades regionales para determinada acción, sino que se la delegan a la autoridad de cada país[1], de modo que en lo que se refiere a temas de carácter penal, y por consiguiente a protocolos criminalísticos, se utilizarían las normas internas de cada país, con salvedad de que exista una norma supranacional que regule una determina situación jurídica.

[1] Un claro ejemplo de esto se encuentra por en la lucha contra los delitos de biopiratería, que se regulan en la Decisión 486, en la cual, no se crea una autoridad de la CAN para perseguir y sancionar estas acciones, sino que delega a la autoridad competente en materia de propiedad intelectual de cada país miembro, que sea la que ejerza las acciones dispuestas en la normativa de la CAN, de acuerdo con los principios de territorialidad donde se haya cometida la infracción.

Precisamente en este sentido, el segundo punto importante que requiere explicarse, es que ninguno de los países miembros de la CAN, con salvedad de la República del Perú, poseen un protocolo, manual, o metodología de trabajo en materia de análisis pericial informático. Tampoco, La República del Ecuador, La República del Perú y la República Plurinacional de Bolivia, han adoptado oficialmente el modelo de Manual de Manejo de Evidencias Digitales y Entornos Informáticos de la Organización de Estados Americanos u otros organismos internacionales.

Por esta razón, la presente Metodología de Trabajo del Sistema Pericial Informático, ha sido desarrollada, en primer lugar, para cubrir el vacío normativo de la legislación penal y criminalística ecuatoriana, que no posee ningún instrumento protocolario de actuación para los peritos informáticos, siendo una necesidad urgente, considerando el incremento de los delitos informáticos en todo el mundo; pero al mismo tiempo, el mismo servirá como una ley modelo para los demás países miembros de la CAN que tampoco poseen una normativa concreta que regule estos aspectos.

En tal sentido, las Decisiones de la CAN suelen tan solo utilizar términos genéricos en lo referente a las autoridades y particularidades de la legislación de cada país; es decir, en vez de señalar que: “el Fiscal dirigirá la investigación penal” establece que: “la investigación penal está a cargo de la autoridad nacional de dirección de la investigación de cada país”, y que la misma “se efectuará con base a los órganos auxiliares de investigación criminológica nacionales”, sin establecer el nombre propio de este organismo en cada país (Por ejemplo Policía Judicial o Sistema de Ciencias Forenses).

Sin embargo, debe especificarse que los países miembros de la CAN, guardan gran semejanza en sus legislaciones internas penales, por lo que en el proceso penal, solo cambian aspectos formales como los nombres de las autoridades u organismos de la investigación, los nombres de las etapas penales, los tipos penales informáticos, entre otros aspectos; pero claramente estos aspectos no influyen de manera directa al momento de establecer una legislación comunitaria andina para la pericia informática.

De esta manera, se considera que la presente metodología de trabajo constituye una importante oportunidad para crear una Metodología de Trabajo del Sistema Pericial Informático aplicable a la mayoría de países de la CAN, con salvedad de la República de Perú, que tiene su propio Manual de Evidencia Digital, en cuyo caso, solo se requeriría armonizar los preceptos entre los dos instrumentos para que exista una cooperación andina eficaz en materia de investigación de los delitos informáticos, que permita investigar y contribuir a la sanción de los delitos informáticos trasnacionales cometidos dentro de los países miembros de la CAN.

7.2 Descripción de la metodología

Metodología de Trabajo del Sistema Pericial Informático

Marco procesal e institucional

1. **Nociones Generales**

- **Definición de Perito**

El Artículo 221 del Código Orgánico Integral Penal (En adelante COIP) define al Perito como "la persona natural o jurídica que por razón de sus conocimientos científicos, técnicos, artísticos, prácticos o profesionales está en condiciones de Principios de actuación informar a la o al juzgador sobre algún hecho o circunstancia relacionado con la materia de la controversia"; y solamente aquellas personas que hayan sido acreditadas por el Consejo de la Judicatura conforme se dispone dentro de este mismo artículo, podrán actuar como tales en los procesos judiciales en distintas materias que requieran la labor pericial.

- **Definición de Perito Informático**

El Perito informático es el encargado de recolectar, preservar, analizar y presentar datos que han sido procesados de forma electrónica y almacenados de forma digital. Su principal objetivo es dar respuesta a preguntas básicas: qué se ha alterado, cómo y quién ha sido el responsable. Para su acreditación, se deberán seguir las normas generales de los peritos en general.

- **Definición de delito informático**

El autor Miguel Davara Rodríguez define el delito informático de la siguiente manera:

> "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 (…) Nos estamos refiriendo solamente, a la comisión de un delito por medios informáticos o telemáticos, ya que la comisión de otros delitos en los que alguna forma interviene un elemento informático, se encontrará sin duda dentro del Derecho Penal General" (Davara, 2008, pág. 358).

2. Marco Procesal

Los peritos informáticos actuarán en el procedimiento penal, cuando existan la presunción de que se ha cometido un delito informático tipificado en el COIP dentro de los “Delitos contra la seguridad de los activos de los sistemas de información y comunicación”, a petición del fiscal, quien es el titular de la acción penal en la fase de investigación previa y en la fase de instrucción, cuando el mismo considere que se requiere contar con un profesional que ayude con sus conocimientos en el campo informático, para averiguar, interpretar o comprobar información contenida en soportes informáticos que constituyan indicios, elementos de convicción o evidencias dentro de la investigación del delito.

En cuanto a la labor del perito, básicamente la misma se completará dentro de tres etapas:

a) Examinación de la evidencia

b) Elaborar un informe pericial

c) Declaración en el proceso penal

3. Principios de Actuación pericial

a) Dirección del procedimiento

De acuerdo con lo previsto en la Constitución de la República y el COIP; siendo el Fiscal quien dirige la investigación del delito, será el quien disponga el tipo de pericias informáticas a realizarse, estableciendo las directrices generales del procedimiento y las cuestiones a esclarecerse con los indicios y elementos de convicción informáticos que se han encontrado y que han sido entregados a los peritos siguiendo la cadena de custodia dispuesto en el Manual de Cadena de Custodia del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses.

b) Imparcialidad

Si bien es cierto, el Fiscal es quien dirige la investigación pre procesal y procesal penal, la información que se encuentre dentro indicios y elementos de convicción informáticos deberá ser analizada de manera imparcial por el perito, estableciéndose las conclusiones respectivas de acuerdo con el nivel de conocimiento de la ciencia informática y no a los intereses de las partes.

c) Deber de reserva

Según lo dispone el COIP, la etapa de investigación pre procesal e instrucción fiscal son reservadas, de modo que la información obtenida de las pericias informáticas, deberá ser reservada. De igual manera, se reservará la información de los delitos en los cuales, debido a su naturaleza, se deba guardar reserva de la información, como delitos sexuales o contra la seguridad del Estado.

d) Límites legales

Los indicios y elementos de convicción informáticos deberán ser analizados, siempre que se haya seguido la cadena de custodia y también cuando exista autorización judicial para realizar las diligencias. En los casos en los cuales las diligencias periciales den indicio de nuevos delitos, deberán ser notificados al Fiscal del proceso.

4. Desarrollo de las Etapas

4.1 Examinación de la evidencia

La Examinación de la evidencia se desarrollará en las siguientes fases:

a) Realización de actos y formalidades iniciales

Con anterioridad a dar inicio a la elaboración de la pericia, el perito informático deberá realizar los siguientes actos:

- Se reunirá con el fiscal del caso para la determinación de los puntos de la tarea pericial a efectuarse.
- El perito informático deberá informarse acerca del tipo penal que se está investigando, el tipo de pericia informática que se realizará, y el objeto y propósitos de la misma, para lo cual podrá solicitar al Fiscal la información necesaria.
- Diseñar la estrategia de la pericia informática investigativa a realizarse, tendiente a lograr evidencias que ayuden al fiscal a determinar la materialidad de la investigación.
- Solicitar el examen de otras las actuaciones o actos investigativos o procesales que considere pertinentes o necesarios para su labor pericial.
- Solicitar al fiscal determinadas acciones, pruebas o informes necesarios para realizar la pericia informática solicitada, como reportes de proveedores de servicios de internet, telefonía, almacenamiento de datos, contraseñas, validación del origen, validación de la integridad de dispositivos, cooperación internacional, entre otros.

- Si existieran diversas tareas a su cargo, el perito informático deberá solicitar al Fiscal que establezca el nivel de prioridad de cada diligencia y también deberá informar al Fiscal del tiempo estimado de cada diligencia pericial.

- Preguntar al fiscal acerca de las dudas que tenga de los límites legales acerca de la pericia informática a realizarse.

- El perito informático deberá asegurarse de contar con las herramientas técnicas, software y hardware y equipos necesarios para realizar la pericia informática, caso contrario, deberá solicitar un laboratorio externo al Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses para completar la diligencia.

- El perito informático solicitará al fiscal la información acerca de la existencia de otros peritos que estuvieren realizando otra pericia informática en el mismo caso, para establecer la debida coordinación de ser el caso.

- El perito informático solicitará al fiscal la información acerca de los peritos que estuviesen autorizados para intervenir, auxiliar u observar la pericia informática a realizarse.

- El perito informático deberá notificar el inicio de las tareas periciales mediante acta, dejando constancia acerca del respeto de cadena de custodia.

b) Preparación del análisis

Como su denominación lo indica, la fase de preparación tiene como finalidad realizar todos los procedimientos previos necesarios para elaborar la pericia informática, para lo cual es imprescindible crear el entorno de pruebas necesario para que se puedan llevar a cabo las actividades de inspección, recuperación y análisis de la información. En esta fase se llevarán a cabo las siguientes tareas:

- Obtención de datos forenses, para lo cual procederá con su extracción de los medios de almacenamiento pertinentes que le han sido entregados al perito forense, respetando la cadena de custodia. Para que los datos forenses sean restaurados se deberá realizar las actividades necesarias, como el montaje en una unidad de disco, iniciándola dentro de una máquina virtual o a través del uso de una suite de herramientas disponibles para el análisis forense. Si fuera necesario, se realizará después del ensamblado, la descompresión de las distintas divisiones de los datos forenses.

- Restauración de datos forenses propiamente dicha, procedimiento en el cual se deberá controlar la confiabilidad de la evidencia recibida. Este proceso será especialmente minucioso, cuando la evidencia entregada para el examen haya sido remitida por terceras personas, ya sean las víctimas, empresas proveedoras de servicios o de cooperación con autoridades de otras jurisdicciones nacionales o internacionales, entre otras. En este caso, se deberán formular las respectivas observaciones que se creyeren necesarias, sobre todo en lo relacionado a la acreditación de su origen, el grado de autenticidad de las mismas y la integridad de los datos forenses. Si en la opinión experta del perito, los indicios o elementos de convicción recibidos carecieron del mínimo de confiabilidad que se requiere para realizar el peritaje informático, el mismo deberá notificarlo al fiscal del caso para que tome las acciones que creyere convenientes.

- Realización de una copia de respaldo forense, sobre la cual se deberán realizar las actividades periciales informáticas, a fin de no comprometer la integralidad de la información de los datos originales, para lo cual se deberá dejar constancia de que los datos originales y la copia forense son idénticos, mediante un procedimiento de validación.

- Realización de un examen general de los indicios y elementos de convicción entregados. Siendo éstos, ordenadores, se deberá identificar la cantidad de discos físicos existente, estableciendo sus características, particiones y sistemas de archivos. En el caso de que se traten de unidades de almacenamiento de establecerán las particiones de ser el caso y sus características.

- Realización de un examen general de los datos forenses encontrados, para lo cual se deberá proceder con la identificación de cantidad y tipo de sistemas operativos que se hallen dentro del hardware. También se buscará e identificará las máquinas virtuales que se hallen presentes.

- Realización de actividades de recomposición de Volumen RAID si fuera necesario.

- Identificación de tipos de archivos encontrados en ordenadores y unidades de almacenamiento externas.

- Identificar de medios de encriptación si los hubiera e inicio de proceso de des encriptación.

c) Análisis Pericial Informático

Constituye una de las etapas más importantes de la pericia informática, ya que en la misma es donde se analiza el contenido de los datos forenses, en busca de evidencias o vestigios que se pretenda encontrar, para lo cual resulta imprescindible recordar los objetivos de la pericia entregados por el fiscal en el inicio del procedimiento, mismos que servirán de base para la realización del análisis forense, sin perjuicio de otros datos que se pudieren encontrar y que se consideren también como información relevante, como de la que se pudiere deducir la existencia de otros delitos. Esta fase comprende las siguientes tareas:

- Extracción Lógica. Se realizará mediante la utilización del sistema operativo del mismo equipo cuando se traten de ordenadores o mediante el uso de un ordenador del laboratorio en el caso de los medios de almacenamiento, para lo cual se emplearán las herramientas de extracción del mismo sistema, determinando la información de los datos existentes respecto a su creación o incorporación en el sistema, el usuario responsable de esta acción y la forma en la cual los mismos han sido utilizados. Este tipo de extracción comprende principalmente las siguientes acciones:

    - ✓ Recuperar archivos eliminados.
    - ✓ Extraer Información de acuerdo con el tipo de archivo a examinarse
    - ✓ Extraer metadatos del archivo.
    - ✓ Desbloquear archivos protegidos con contraseña.
    - ✓ Descomprimir archivos comprimidos mediante utilización de software

- ✓ Des encriptación de archivos encriptados mediante utilización de software
- ✓ Identificación y documentación de la Información de configuración.

- Extracción Física, Se realizará de manera directa en los datos forenses presentes en el disco, con el objeto de hallar archivos que hayan sido borrados de manera parcial o total, o archivos ocultados mediante el uso de programas, herramientas informáticas, y que con el sistema operativo no se hayan podido detectar. Para este efecto se utilizarán programas informáticos adecuados. Se buscará la información dentro del disco duro u otras unidades de almacenamiento, aun dentro de los espacios no asignados.

d) Interpretación

Es otra de las fases de investigación más importantes de la pericia informática, es la interpretación, y en la que el perito informático debe aportar en mayor forma con su conocimiento técnico, ya que esta podría ser considerada la fase con una mayor carga subjetiva, frente a las anteriores que resultan eminentemente objetivas.

En este sentido, una vez que se halle información que pudiere ser potencialmente relevante para la investigación del tipo penal o que brindare información acerca de cometimiento de otro tipo de delitos, el perito informático tendrá la obligación de interpretar la información en la mejor forma posible, de acuerdo con su conocimiento y de manera pertinente en el caso, de acuerdo con los puntos de la tarea pericial encomendada por el fiscal.

Antes de realizar la interpretación, el perito informático deberá realizar un proceso de selección y clasificación de la información recolectada, establecido el orden la información de acuerdo al grado de relevancia para la investigación penal. También se deberá evaluar la amplitud de la información para poder establecer si se cumplirá con el cronograma entregado al fiscal, o si, por el contrario, se requerirá de una ampliación del mismo. Se podrá pedir la asistencia del fiscal para que determine los criterios selección de evidencia de acuerdo a la necesidad de la investigación penal.

También se deberá clasificar la información concerniente al cometimiento de otro tipo de delitos o la que pudiere resultar sensible respecto de terceras personas que requiera ser protegida.

La interpretación del perito informático deberá contener principalmente los siguientes datos:

- Descripción de los dispositivos de hardware encontrados en el ordenador y las funciones que desempeñaban los mismos
- Identificar el software instalado en los ordenadores y describir sus funcionalidades; así como el uso que le daba el usuario, para lo cual se deberá analizar el código fuente, los programas, aplicaciones utilizados y los archivos utilizados o exportados por estas aplicaciones y programas que se hallen en el escritorio del ordenados, en los dispositivos móviles o en sitios web de almacenamiento.
- Analizar cuáles fueron los sitios web visitados por el usuario y los servicios en línea utilizados, estableciendo el grado de frecuencia de uso.
- Clasificar, los datos informáticos encontrados y relacionarlos con los criterios establecidos para la realización de la pericia.
- Identificar los archivos con características específicas que hayan sido solicitadas por el fiscal como relevantes para la pericia.
- Realizar la reconstrucción de líneas de tiempo, en cuanto a la creación, alteración, acceso, reproducción, envío, recibimiento, o eliminación de archivos, o también de accesos y salidas de usuarios de los programas y aplicaciones informáticos y sistemas operativos.
- Identificar las transacciones electrónicas realizadas por el usuario.
- Reconstrucción de rutas de información.

Otras actividades propias de la interpretación que realizará el perito informático son las siguientes:

- Detección de patrones de los usuarios sospechosos.
- Elaboración de hipótesis con base en la información obtenida
- Identificación de *modus operandi* de determinados delitos
- De contar con la información necesario se podría realizar la individualización de un usuario que haya realizado determinadas actividades, estableciendo posibles autores, o cómplices del delito.

Finalmente, de ser necesario, se incluirá en el informe la actuación que se hubiera poder realizado de manera conjunta con otros peritos, cuando esta labor hubiere sido interdisciplinaria con peritos expertos de otras áreas, ya sean dentro del ámbito informático u otras distintas a esta, o aquella derivada de la cooperación internacional con otros peritos.

También se deberá hacer constar, los alcances y limitaciones que tuvieron para el desempeño de su labor, sugiriendo posibles diligencias o pericias que consideren pertinentes para corroborar o complementar su labor realizada.

4.2 Elaboración de un informe pericial

De acuerdo con lo previsto dentro en la legislación ecuatoriana, el informe pericial cumplirá con las normas mínimas establecidas en el Código Orgánico Integral Penal siendo los requisitos mínimos: Antecedentes, Consideraciones Técnicas, Metodología Empleada, Conclusiones y Anexos.

En cuanto a la redacción del mismo, debe considerarse que el mismo deberá se comprensible tanto para las personas conocedoras de la materia informática, como para las no expertas en el campo, de modo que deberá ser claro y comprensible, pudiendo acompañarse de imágenes que ayuden en este propósito. Respecto al contenido mínimo que deberá tener el informe pericial informático, el mismo será:

Antecedentes. - Contendrán los siguientes elementos:

- Objeto de la pericia.
- Descripción de los elementos recibidos y sus condiciones.
- Datos relacionados con la cadena de custodia

Consideraciones Técnicas. - Contendrán los siguientes elementos:

- Herramientas y técnicas utilizadas
- Operaciones practicadas

Metodología Empleada. - Contendrán los siguientes elementos:

- Justificación de los métodos empleados
- Lugar y fecha de las actividades realizadas
- Principios de la ciencia informática a utilizarse

Conclusiones. - Contendrán los siguientes elementos:

- Resultados obtenidos
- Hallazgos obtenidos
- Margen de error
- Limitaciones
- Observaciones que se consideren pertinentes

Anexos. - Contendrán los siguientes elementos:

- Gráficos
- Imágenes
- Datos en formato digital que se consideren relevantes.

4.3 Declaración en el proceso penal

Conforme se dispone en las normas procesales, el perito informático tendrá la obligación de comparecer personalmente a la audiencia de juicio para presentar sus explicaciones y aclaraciones de forma verbal.

El perito deberá ser capacitado para la declaración en el proceso penal, para lo cual se deberá acreditar en primer lugar su experiencia, objetividad y cumplimiento de las normas procesales y de la presente metodología de trabajo, debiendo instruirle con conocimiento básicos del proceso penal.

Asimismo, el fiscal podrá solicitar una reunión con el perito previo al procedimiento penal, con el fin de capacitarle en cuanto a su declaración en el caso, principalmente en lo que se relaciona con la relevancia de los hallazgos que se mencionaran en el proceso penal, la forma en la que realizará su exposición (didácticamente y comprensible),la objetividad que deberá tener, los lineamientos del interrogatorio a efectuarse, la secuencia de su exposición, las cuestiones acerca de las cuales no debería declarar (las que están fuera de su incumbencia o que son ajenas a su campo de saber), la forma en la que debe aclarar y ampliar su exposición.

5. Fin de la pericia

La finalizar la pericia y una vez elaborado el informe, el perito continuará con la cadena de custodia de los indicios y elementos de convicción informáticos que fueron objeto de la pericia, para lo cual, se aplicará lo dispuesto en el Manual de Cadena de Custodia del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses que dispone la forma en la cual los mismos serán almacenados hasta que se realice la audiencia de juicio, y posteriormente se dispone que: “El destino final de los indicios y/o evidencias, únicamente será dispuesto por la o el Fiscal o la o el Juez competente, lo cual debe hacerse por escrito mediante resolución, y siguiendo el respectivo registró en los documentos propios para este efecto”.

6. Anexos.

En cuanto a la actuación de los peritos informáticos dentro de la escena del delito, se aplicarán los procedimientos dispuestos dentro del Manual de Cadena de Custodia del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses que se reproduce a continuación:

> **“Procedimiento en indicios y/o evidencias digitales**
>
> Las Unidades del Sistema Especializado Integral de Investigaciones, Medicina Legal y Ciencias Forenses que lleguen al lugar de los hechos con fines de aplicación metodológica para procesar los dispositivos informáticos y electrónicos, primero deben observar, buscar, fijar y levantar indicios biológicos como: A.D.N., huellas dactilares latentes, entre otros. En caso de interceptación de comunicaciones, indicio y/o evidencia digital, una vez concluida la investigación deberá ser entregada a un centro de acopio del sistema, hasta que sea requerido

por la autoridad competente. Cuando la interceptación de comunicaciones se desarrolle como parte de una operación encubierta o entrega vigilada o controlada será conservada con carácter de secreto y mantenida en una sección especial de los centros de acopio del Sistema.

Manejo de la Escena (Territorio Digital)

1. Asegurar inmediatamente todos los dispositivos informáticos o electrónicos dentro de la escena del hecho, a fin de garantizar que no se alteren las condiciones físicas de dichos dispositivos.

2. Mantener el dispositivo informático o electrónico en el mismo estado que se encuentre, apagado o encendido.

3. Levantar rastros de huellas dactilares latentes, A.D.N. u otros, en los dispositivos informáticos o electrónicos, tales como: Teclados, mouse, impresoras, monitores, escáners, PDA y otros.

4. Verificar si el equipo informático o electrónico esta encendido y documentar lo que la pantalla presenta o muestra.

5. Identificar si el equipo está conectado a un sistema de red o internet, debe desconectar el cable para impedir el acceso remoto.

6. Fijar, embalar, sellar y rotular el equipo informático o electrónico en la escena.

7. Transportar el equipo informático o electrónico de una manera segura y confiable.

Metodología si el dispositivo está apagado

1. Documentar descriptiva y fotográficamente los dispositivos y cables conectados al equipo, de acuerdo al instructivo. 2. Individualizar y etiquetar cada uno de los cables y dispositivos que almacenan información digital. 3. Verificar si existen unidades de almacenamiento dentro de los dispositivos como CD, DVD, USB y otros, los cuales deben ser sellados con cinta de seguridad (cinta de evidencias). 4. Registrar el modelo, marca, número de serie, y marcas distintivas del equipo. 5. Sellar con cinta de seguridad (cinta de evidencia) los puertos USB y conector de energía. 6. Observar los protocolos para el tratamiento de este tipo de indicios y/o evidencias.

Metodología si el dispositivo está encendido

1. Documentar descriptiva y fotográficamente los dispositivos y cables conectados al equipo, de acuerdo al instructivo.

2. De ser necesario solicite asistencia del personal especializado con experiencia en captura y preservación de información volátil.

3. Desconectar el cable o batería únicamente en los siguientes casos: a. Si aparece en pantalla que el equipo fue borrado o formateado. b. Si se observa que está en proceso de borrado o formateado el sistema de almacenamiento.

4. No desconectar la batería o el cable de poder cuando:

a. La información que aparece en la pantalla es de trascendental importancia para el proceso investigativo.

b. Cuando en la pantalla se presenta: Redes sociales, salas de chats, comunicación interactiva, almacenamiento de datos remotos, documentos encriptados, documentos abiertos, considerado esto territorio digital Art. 460 Nral. 8 COIP. 5. Observar los protocolos para el tratamiento de este tipo de indicios y/o evidencias.

Embalaje de dispositivos informáticos o electrónicos

El proceso de empaquetamiento debe considerar los siguientes lineamientos técnicos:

1. Todo dispositivo informático o electrónico debe embalarse en fundas y/o recipientes antiestáticos.

2. No se debe usar fundas plásticas que puedan producir estática o permitan humedad y condensación.

3. Los empaques de evidencia digital deben prevenir: Rayones, golpes, movimientos bruscos" (Fiscalía General del Estado, 2017, págs. 13, 14).

8 VALIDACIÓN DE LA METODOLOGÍA

8.1 Descripción del caso

En la ciudad de Quito, se envían 10 correos informáticos a usuarios de un Banco Local, con un mensaje de solicitud de información de nombre de usuarios y contraseña para ingresar al sistema bancario. Una de las personas ingreso la información solicitada, y posteriormente verificó que el dinero que tenía en el Banco fue trasferido a otra cuenta sin su autorización, por lo que denunció el hecho en la Fiscalía ecuatoriana.

El Fiscal, una vez que conoció el caso, abrió una etapa de investigación previa, por el delito de Transferencia electrónica de activo patrimonial, tipificada en el COIP en su artículo 231 que prevé:

> "Artículo 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años."

Posteriormente, ordenó las pericias necesarias, identificándose que el lugar de donde se cometió el delito era una oficina rentada en la ciudad de Guayaquil, ordenando el allanamiento del inmueble, donde se decomisó dos equipos informáticos portátiles, que fueron puestos en cadena de custodia para que fueran analizados por los peritos informáticos, aplicándose el protocolo.

Se determina además que existen conexiones con una empresa ubicada en la ciudad de Bogotá en Colombia, destino a donde se enviaba el dinero, y en donde se contrató un servicio de hosting, por lo que se procede a realizar la cooperación internacional con Colombia, aplicándose por igual el protocolo en los dos países.

El fiscal de Colombia, procede abrir una investigación por el delito de Suplantación de sitios web para capturar datos personales, contemplado en el artículo 269G del Código Penal Colombiano, que prevé:

> "Artículo 269G. Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. 214 En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito".

En la ciudad de Bogotá se allana una oficina donde se decomisa un computador y dinero en efectiva que no se puede justificar, por lo que solicita la realización de la pericia informática, y se solicita la cooperación internacional de Ecuador.

Descripción del análisis

Con anterioridad a dar inicio a la elaboración de la pericia, el perito informático solicita una reunión con el fiscal, quien solicita como puntos de la investigación pericial los siguientes:

- Descripción de los programas informáticos instalados encontrados en los equipos portátiles.
- Descripción de los programas informáticos que hayan sido creados por los usuarios de los equipos portátiles.
- Descripción de los correos electrónicos enviados desde los equipos portátiles.
- Descripción de las direcciones electrónicas visitadas desde los equipos portátiles.
- Descripción de trasferencias bancarias que se hayan realizado desde los equipos portátiles.

El fiscal le señala el perito que la investigación previa es por el delito de Transferencia electrónica de activo patrimonial. El perito solicita al Fiscal que ordené judicialmente al proveedor de internet, el reporte de las direcciones electrónicas visitadas desde los equipos portátiles en el último año, así como que establezca cual es la tarea prioritaria de la pericia, siendo esta la descripción de los programas informáticos que hayan sido creados por los dueños de los equipos portátiles y la descripción de las direcciones electrónicas visitadas desde los equipos portátiles.

El perito solicita al Fiscal que ordené judicialmente al Banco, a fin de que se detallen las trasferencias bancarias que se han realizado desde las cuentas de los usuarios que han sido perjudicados por el hurto del patrimonio de sus cuentas en el banco.

El perito solicita al Fiscal la cooperación internacional con Colombia a fin de poder contrastar la información que se ha obtenido en las pericias realizadas en Colombia.

El perito realiza el acta de inicio de investigación, conforme lo determina el Protocolo y deja constancia de la correcta aplicación de la cadena de custodia.

Preparación del análisis informático

Posteriormente, en aplicación del protocolo, se realiza la preparación del análisis informático, para lo cual, se procede con la extracción de los equipos portátiles, se procede con la extracción de los discos duros, a fin de realizar una copia de respaldo forense.

Se procede con la realización de un examen general de los equipos entregados. Se identifica la cantidad de un disco duro físico existente en cada una de los equipos, sin particiones de discos encontradas, se establecen sus características, como marcas, modelos, capacidad de almacenamiento y sistemas operativos encontrados, programas informáticos, también la cantidad de carpetas y archivos encontrados en los mismos, lo cual se hace constar en el informe.

Análisis Pericial Informático

Posteriormente se procede con el Análisis Pericial Informático, empezando con la extracción lógica, se realizará con la utilización del mismo sistema operativo de los equipos utilizando las herramientas de extracción del sistema.

En este caso, se procede con la determinación de los programas informáticos instalados, siendo 10 programas en total, de los cuales, uno no resulta desconocido, y no tiene información acerca de algún fabricante conocido.

Se detalla la función que tenía este programa, siendo la misma la de enviar correos electrónicos de manera automática con información bancaria y almacenar la información de respuesta de los usuarios.

De determina además cual fue el contenido de los correos electrónicos enviados desde los equipos portátiles.

Se analizan cuáles han sido las direcciones electrónicas visitadas desde los equipos portátiles, entre las que se encuentra un sitito que ha sido creado por los mismos usuarios, según se observa en los correos electrónicos recibidos. El hosting de esta página web se encuentra en la ciudad de Bogotá.

Se determina que este sitio web, es una réplica del sitio del banco, y el mismo tenía como finalidad el almacenar los datos de los usuarios, como nombres de usuarios y contraseñas.

Se realizan también las pericias para determinar los accesos que se han dado al sitio web del banco, con el objeto de poder establecer las trasferencias bancarias que se hayan realizado desde los equipos portátiles.

Se realiza además mediante uso de software especializado y técnicas convencionales, el detalle de la recuperación de archivos que se han eliminado.

Se procede con el desbloqueo de archivos protegidos con contraseña.

Interpretación del perito informático

La interpretación del perito informático empieza con la descripción de los dispositivos de hardware encontrados en el ordenador y el establecimiento de las funciones que desempeñaban los mismos.

Se realiza la Identificación del software instalado en los ordenadores y describir sus funcionalidades; centrándose principalmente en el programa informático que fue creado y de los sitios web creados y visitados, señalando también la frecuencia de uso.

Se clasifica los datos informáticos encontrados y se relaciona con los criterios establecidos para la realización de la pericia.

Se procede a realizar la identificación de los programas, sitios web y archivos con características específicas que son relevantes en la pericia.

Se realiza la creación de una línea de tiempo, con los datos de creación, alteración, acceso, reproducción, envío, recibimiento, o eliminación de archivos, o también de accesos y salidas de usuarios de los programas y aplicaciones informáticos y sistemas operativos, para lo cual también se utiliza la información recibida del proveedor de internet.

Se realiza la identificación de las transacciones electrónicas realizadas por el usuario, con los datos de usuarios y contraseñas que se hurtaron a los usuarios, para lo cual, se utiliza la información que ha sido solicitada al Banco.

Finalmente, se realiza la elaboración de hipótesis con base en la información obtenida en la pericia, estableciendo el *modus operandi* de los delitos cometidos. Se procede con la individualización de las actividades realizadas, estableciendo a los posibles autores o cómplices del delito, con base en los perfiles de las personas que realizaron las actividades determinadas en las pericias.

Informe pericial

Se procede con la elaboración de un informe pericial, mismo que contiene la siguiente información:

Antecedentes. - Contendrán los siguientes elementos:

- Objeto de la pericia.
- Descripción de los elementos recibidos y sus condiciones.

- Datos relacionados con la cadena de custodia

Consideraciones Técnicas. - Contendrán los siguientes elementos:

- Herramientas y técnicas utilizadas
- Operaciones practicadas

Metodología Empleada. - Contendrán los siguientes elementos:

- Justificación de los métodos empleados
- Lugar y fecha de las actividades realizadas
- Principios de la ciencia informática a utilizarse

Conclusiones. - Contendrán los siguientes elementos:

- Resultados obtenidos
- Hallazgos obtenidos
- Margen de error
- Limitaciones
- Observaciones que se consideren pertinentes

Anexos. - Contendrán los siguientes elementos:

- Gráficos
- Imágenes
- Datos en formato digital que se consideren relevantes.

Declaración en el proceso penal

Se solicita al Fiscal una reunión, a fin de establecer los puntos más importantes que se deberán exponer en la declaración en el proceso penal.

8.2 Aporte de la metodología en el caso de estudio

En el caso antes descrito, se observa la dinámica en la cual se pueden presentar los delitos informáticos, en muchos casos, los mismos suelen superar la territorialidad de los Estados, presentándose considerables dificultades para poder judicializarlos, pero sobre todo también para poder investigarlos de una manera adecuada.

En este sentido, debe mencionarse que diversas legislaciones en América Latina, y particularmente en el caso de la Comunidad Andina de Naciones, no tienen protocolos estandarizados de investigación pericial informática, lo cual puede perjudicar seriamente al momento de la investigación y judicialización penal de los distintos tipos penales informáticos; ya que al no existir estándares mínimos para este tipo de pericias, que por su naturaleza jurídica compleja y principalmente técnica, se puede generar impunidad, en el sentido de que una investigación mal desarrollada, no cumplirá con los objetivos del proceso penal, que son la determinación de la existencia material de un delito y la demostración del nexo causal con el presunto infractor, así como tampoco se podría garantizar los principios universales del debido proceso.

Por esta razón, se considera de gran importancia el desarrollo de la presente metodología de trabajo para el perito informático, que debe realizar su experticia dentro de los países pertenecientes a la CAN, pues de esta manera, se estandariza el método de trabajo que deben usar los peritos para avalar su investigación, tanto a nivel nacional, como a nivel internacional, en el caso de que se requiera cooperación o asistencia internacional para la investigación de un delito informático.

La metodología de trabajo del sistema pericial informático además se constituye como un importante instrumento de capacitación para los peritos de los países de la CAN, pues debe considerarse que la investigación penal constituye una labor conjunta entre las diversas disciplinas de la ciencia criminalística (entre ellas la pericia informática) y la ciencia jurídica; y esta segunda, no es de conocimiento general por parte de un especialista en materia informática; de allí que se requiera capacitarle en los aspectos generales del proceso penal, como el marco legal procesal en materia penal, así como también de los principios de actuación pericial que se requieren cumplir.

En este sentido, también se requiere que el perito informático tenga conocimiento acerca de la realización de actos y formalidades iniciales propios del proceso penal y la investigación pre-procesal, como aquellos que están relacionados con la aplicación y respeto de la cadena de custodia y el manejo de la evidencia digital; así como la coordinación que se debe tener con el Fiscal del caso, que según dispone la normativa penal, es quien dirige la investigación, ordenando las diligencias que deben practicarse, así como también la prioridad que tienen las mismas.

Ya en lo que se refiere al análisis pericial propiamente dicho, si bien es cierto, el perito informático es experto en la realización de este tipo de diligencias, la metodología de trabajo le permite que la pericia sea realizada de manera sistematizada y ordenada, de modo que desde la preparación del análisis, el análisis pericial Informático propiamente dicho y la interpretación, puedan ser realizados de acuerdo con las exigencias de la normativa, lo que permitirá que las pericias puedan ser validadas dentro de todo los países del área andina, lo que no sucedería en el caso de no existir una metodología de trabajo comunitaria, pues la divergencia de requisitos haría necesario más de una pericia informática, de acuerdo con las exigencias de cada Estado.

La correcta estructuración de la metodología de trabajo del sistema pericial informático además reviste de validez científica a este proceso, pues se contemplan las principales fases y actividades que se requiere para la demostración material de hechos con base en los principios de la lógica y de la ciencia, lo que permitirá que esta labor pericial pueda ser validada dentro de un proceso penal, tanto por la fiscalía, la defensa del procesado y también por el juez o tribunal que conocen la causa.

Así también el aporte de la metodología de trabajo del sistema pericial informático del proceso penal está en que se legitimará la actuación del perito en las etapas posteriores a la realización de la pericia, que empezarán con la correcta elaboración del informe pericial, que deberá contener todos los puntos relevantes que permitan que este instrumento sea validado y aceptado, permitiendo demostrar hechos tendientes al descubrimiento de la verdad material de los hechos.

Finalmente, en el desarrollo de la metodología se observa como esta contribuye en la capacitación de los peritos, para que puedan realizar una correcta declaración en el proceso penal, que se logrará con la asistencia del fiscal, ya que la pericia por sí misma no constituye un medio de prueba determinante, sino está acompañada del testimonio del perito, que permitirá una mejor comprensión, aclarará las posibles dudas e interrogantes que se presenten, pero sobre todo, se podrá cumplir con los principios de inmediación y contradicción de la prueba exigidos en el proceso penal.

Como se observa, existen muchos aportes de la metodología de trabajo del sistema pericial informático para la CAN, ya que de no incorporarse la misma, la investigación del delito informático se podría realizar de manera desorganizada, no estandarizada y no avalada conforme a los principios de la ciencia informática, lo que será perjudicial para la investigación del proceso penal, una situación que debe ser corregida de manera prioritaria dentro de la CAN, en virtud del aumento de los delitos informáticos que se ha dado en la actualidad, siendo necesario que también las instituciones de persecución criminal, tomen medidas de mejora la investigación y sanción de estos delitos.

9 CONCLUSIONES

A través del desarrollo del presente trabajo de investigación se ha llegado a las siguientes conclusiones:

- El delito informático constituye un término dinámico, en razón de que se adapta no solo a un tipo penal en concreto, sino que al contrario, el mismo puede presentarse en diversas conductas delictivas que afectan a diversos bienes jurídicos protegidos, y cuya característica en común, es el uso del computador como medio o instrumento para materializar esta infracción, de allí que existan algunos criterios doctrinarios que consideren que no se tratan de un grupo de delitos nuevos, sino más bien de delitos ya tipificados, pero que tiene una nueva forma de cometerse, mediante el uso de las tecnologías de la información.

- Respecto al sujeto activo del delito de la infracción del delito informático, es su persona que tiene gran habilidad para dominar los sistemas informáticos, y muchas veces son los trabajadores de empresas quienes cometen estas acciones delictivas al interior de sus propios lugares de trabajo, esto debido a la posibilidad de anonimato que recibe el internet. En cuanto a los sujetos pasivos del delito, son las personas que sufren las afectaciones de la infracción penal, quienes pueden ser personas naturales o jurídicas, inclusive organismos pertenecientes al mismo Estado.

- En el caso del bien jurídico protegido, debe resaltarse que los delitos informáticos se tratan de delitos pluriofensivos o complejos, debido a que constituyen una serie de conductas que coinciden con varias figuras penales tradicionales, razón por la cual, no existe un solo bien jurídico protegido afectado, sino varios, principalmente el patrimonio y propiedad; también se afecta el derecho a la intimidad y confidencialidad de los datos y la seguridad e inclusive la afectación puede recaer en la afectación de otros delitos más graves contra la integridad física, psicológica y sexual de la persona.

- Dos de las características más importantes de los delitos informáticos son la transnacionalidad, ya que este delito permite que el delincuente este muy alejado de la víctima, inclusive en otro país, de allí que se considere que esta clase de infracciones no reconozca las fronteras geográficas, pues se desarrolla en su mismo universo ilimitado. Esto conlleva a la segunda característica, y es que se tratan de delitos que tiene una desventaja para la persecución del delito, pues las instituciones de persecución criminal si obedecen a una lógica de territorialidad, requiriéndose de

cooperación internacional para poder sancionar a los infractores. Esto sin duda es una ventaja para el delincuente, quien escoge aciertos países para delinquir, donde no existe legislación que permita sancionarlo y así quedar en la impunidad de manera que la investigación de este tipo de delitos se muy compleja, de allí que se requiere de un marco normativo adecuado y también de personal altamente capacitados en la investigación de estos delitos, pues de ello dependerá que los mismos sean sancionados de manera adecuada.

- El Derecho y las Tecnologías de Información y Comunicaciones (TIC), son disciplinas que pertenecen a ámbitos distintos, el primero estudia la regulación de la conducta humana en la sociedad; y las segundas son un conjunto de servicios, aplicaciones y herramientas tecnológicas que van cobrando mayor relevancia a la hora de acceder a la información y al conocimiento en todos los ámbitos de la vida moderna. Sin embargo, estas nuevas tecnologías son utilizadas para cometer delitos, tal es el caso de robos, extorsiones, fraudes y otros tipos de hechos ilícitos a través de los medios electrónicos. De ahí nace la necesidad de contar con personas que tengan la experticia para buscar las evidencias que contribuyan a sancionar estos delitos, este profesional es conocido como Perito informático. Son los encargados de recolectar, preservar, analizar y presentar datos que han sido procesados de forma electrónica y almacenados de forma digital.

- El Perito informático es el encargado de recolectar, preservar, analizar y presentar datos que han sido procesados de forma electrónica y almacenados de forma digital. Su principal objetivo es dar respuesta a preguntas básicas: qué se ha alterado, cómo y quién ha sido el responsable. El perito debe ser imparcial, no cometer hecho con dolo, imprudencia o falta de celo al realizar la pericial. Al mismo tiempo, sus aptitudes deben estar avaladas por una institución reconocida. Esto impedirá que la validez de las evidencias sea puesta en entredicho. Cada país contempla una serie de requisitos en función a sus estudios, formación, experiencia y en algunos casos se exige contar con certificaciones específicas, para que un perito pueda ser reconocido y posteriormente pueda realizar su labor, sin embargo, debe destacarse que en lo que se refiere a la investigación criminológica del delito informático en sí mismo, existen algunos retrasos y deficiencias normativas que requerirían ser subsanadas, para de esta manera proteger de manera adecuada a las personas frente a estos hechos delictivos.

- La legislación española es muy rigurosa al momento de designar a los peritos informáticos, pues existe un conjunto de requisitos que son difíciles de cumplir, no siendo solamente necesario el cumplimiento de requisitos de carácter académico, sino que además deberán acreditar que tiene experiencia en la realización de peritajes y posteriormente superar cada uno de los concursos que les permiten acceder a la colegiatura como peritos. En este sentido, debe destacarse que la legislación española constituye un ejemplo y modelo a seguir en otros países, principalmente de Sudamérica, en donde no se disponen requisitos tan complejos y sobre todo tan especializados para poder acceder a realizar pericias dentro del campo informático.

- Los países que forman parte de la CAN, entre los que se encuentra Ecuador, tienen grandes vacíos que existe a nivel regional, es precisamente la falta de normativa en la subregión andina respecto de los delitos informáticos y su persecución, esto pese a la existencia de normativa vinculante para los Estados en otras áreas, pero en lo que se refiere concretamente al delito informático y la cooperación internacional, no se ha realizado un mayor esfuerzo.

- De las normativas de los países miembros de la CAN, es dentro de la legislación peruana en donde se observa que existen requisitos que son más estrictos para poder ser un perito, ya que se requiere de al menos una doble capacitación, no solo en el área en el cual se va a realizar el peritaje, sino que además se exige una colegiatura en materia de pericia, al igual que lo contempla la legislación española.

- Los países que conforman la CAN, tienen una legislación constitucional que protege el debido proceso como un derecho fundamental a ser respetado en los procedimientos penales, lo que implica que se debe respetar todas las garantías de este derecho, lo que incluye el respeto al principio de legalidad de la prueba. También se ha podido evidenciar que, se cuenta con un marco adecuado en la tipificación de los delitos informáticos, por lo que se protegen a los distintos bienes jurídicos a los que afecta el cometimiento de estos ilícitos, de manera que existe una relación entre los delitos tipificados en cada uno de los países. Sin embargo, un aspecto en el cual se ha notado serias deficiencias tiene que ver con la designación de los peritos y los requisitos que se deben cumplir, ya que en ningún caso existe una normativa especializada que trae acerca del perito informático, sino que en los distintos países existe solo un Reglamento que establece condiciones generales para ser perito en cualquier área, pero no se centra en el perito informático como tal. También se observa deficiencias en la capacitación, pues dentro de la legislación española es requisito

indispensable que, además de acreditar la formación académica en el área científica, se acrediten estudios en centros de formación de peritos o en ciencias criminológicas, requisito que se omite en los países de la CAN.

- Dentro de la normativa argentina, se observa cómo se requiere una doble acreditación para realizar la actividad pericial, ya que Poe una parte se requieren de los conocimientos científicos dentro del área a realizar la pericia, y por el otro, haber tenido alguna formación o capacitación como perito, aunque tampoco se señala de manera específica cual será la formación del perito informático, sino que los mismos se dan de manera general para los profesionales de todas las áreas

- En la la legislación de México se presenta un mayor avance en cuanto a la actividad pericial que en los países sudamericanos, sobre todo en lo que se refiere al criterio de selección de los peritos y de los requisitos que tienen una mayor exigencia al momento de seleccionar al persona pericial, solicitando no solo una formación como profesionales en la distintas áreas, sino que además se busca que exista una formación criminológica o pericial, dentro de las distintas capacitaciones que se realizan incluiste pro parte de organismos estatales.

- En lo que se refiere a la legislación en contra de los delitos informáticos, una de las legislaciones más importantes y desarrolladas es la estadounidense, ya que tiene una gran experiencia en temas de seguridad informática, así como organismos especializados dedicados a la lucha contra los ataques informáticos; pero en el sistema norteamericano, no es suficiente que el perito cumpla una serie de requisitos para poder declarar como un testigo experto, principalmente en cuanto a su capacitación académica o como criminólogo y el tiempo que se ha dedicado a ejercer su actividad como profesional, sino que además se deberá demostrar que su participación dentro del procedimiento penal se encuentra plenamente justificada, y estos aspectos derivan del sistema normativo del *common low* que se diferencia de manera sustancial del derecho romanístico.

- Desde el punto de vista del derecho internacional, se puede afirmar que no existe un tratado internacional que regule toda la actividad de los delincuentes informáticos y se los sancione de manera adecuada, aplicando un principio de territorialidad; sin embrago, con el paso del tiempo se han ido dando importantes avances en materia de protección internacional en contra de los delitos informáticos, existiendo actualmente un conjunto de instrumentos internacionales que permiten la adhesión libre que

permita una mayor cooperación internacional para combatir a los delincuentes informáticos. Por esta razón, es importante que todos estos instrumentos se vayan ampliado y universalizando, con el objetivo de que no se afecten los derechos de las personas, pues solo así se logrará una protección efectiva frente a los mismos, ante una amenaza que es cada vez mayor, y se va incorporando en la sociedad.

- Dentro de la legislación ecuatoriana, los protocolos de investigación del delito a través de las distintas disciplinas científicas que componen la criminalística, no han sido desarrollados de manera eficaz y de acuerdo con los estándares de investigación científica internacional que se requieren para la efectividad de este proceso. Es así, que en lo que se refiere a las pericias de investigación de delitos informáticos, no existe un protocolo de actuación idóneo, pese a la gran importancia que tiene la investigación de estos delitos en la actualidad, que se han incrementado de manera considerable en el Ecuador y en también en todo el mundo. Por lo que la propuesta de comparación normativa, ha podido evidenciar la existencia de diversos vacíos legales en lo referente al perito informático y la investigación de este tipo de delitos, razón por la cual es necesaria la creación un protocolo modelo idóneo para la investigación de delitos informáticos, que pudiere orientar la actuación del perito informático en el Ecuador, esto sin perjuicio de que a nivel de la Comunidad Andina también se cree un protocolo internacional de cooperación multilateral.

10 REFERENCIAS BIBLIOGRÁFICAS

Acurio, S. (2006). *Delitos Informáticos: Generalidades.* San José: Organización de Estados Americanos.

Aguirrezabal, M. (2012). Algunos aspectos relevantes de la prueba pericial en el proceso civil. *Revista de Derecho Universidad Católica del Norte,*, 335-351.

AndalucíaCERT . (2017). Informe de divulgación Phishing. *Seguridad y Confianza Digital*, 1-22.

Anti-Phishing Working Group. (2019). Phishing Activity Trends Report. *Quarter. Most, (March)*, 1-12.

Cárdenas, G. (2015). Ciberacoso. *¿Cómo ves?*, 10-14.

Davara, M. (2008). *Manual de Derecho Informático.* Pamplona: Thomson Aranzadi.

Díaz, M. (2009). Delitos contra la propiedad intelectual e industrial. Especial atención a la aplicación práctica en España. *Revista de Derecho Penal y Criminología*, 9-134.

Estrada, R., & Somellera, R. (1998). Delitos Informáticos . *Revista iberoamericana de derecho informático*, 423-441.

Forensic. (2018). Forensic. *Peritos judiciales en francia,una profesión muy valorada*, Forensic.

Goodman, M. (2016). *Crímenes futuros: dentro del subsuelo digital y la batalla por nuestro mundo conectado .* Nueva York: Transworld.

Lima, M. (1984). *Delitos Electrónicos en Criminalia.* México D. F.: Porrúa.

Mariño, A. (2003). *Responsabilidad Contractual por utilización indebida de tarjeta de crédito.* Barcelona : Tesis doctoral de la Universidad Autónoma de Barcelona.

Mazuelos, J. (2007). Consideraciones sobre el delito de daños informáticos en especial sobre la difusión de Virus Informático. *Revista Jurídica de la Universidad Externado de Colombia*, 29-36.

Molina, J. (2003). *Delitos y otros ilicitos informáticos en el Derecho de la Propiedad Industrial.* México D.F.: Porrúa.

Organización de Naciones Unidas. (2010). *Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente.* Viena: Naciones Unidas.

Organización de Naciones Unidas. (2013). *Estudio exhaustivo sobre el delito cibernético.* Nueva York: UNODC.

Parker, D. (1989). *Crimen informático Manual de Recursos de Justicia Penal.* Washington D.C: Instituto Nacional de Justicia.

Resio, M. (2018). Parada, Ricardo; Errecaborde, Daniel. En D. s. digital, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet* / (págs. 121-131). Buenos Aires : Erreius.

Reyes, A. (1981). *La Tipicidad.* Bogotá: Universidad de Externado de Colombia.

Rodríguez, A. (2014). Análisis económico de la responsabilidad bancaria frente a los fraudes electrónicos el riesgo provecho, el riesgo creado y el riesgo profesional. *Vniversitas*, 285-314.

Romeo, C. (1988). *Poder Informático y Seguridad Jurídica.* Madrid: Fundesco.

Téllez, J. (2003). *Derecho informático.* México D.F.: Mc Graw Hil.

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características …. En R. Parada, & J. Errecaborde, *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet* (págs. 49-68). Buenos Aires: Erreius,.

11 ANEXOS

11.1 Anexos 1 Posibles evidencias a encontrarse en medios tecnológicos

Archivos a encontrarse dentro de la pericia dentro del disco rígido

- ✓ Archivos de usuarios.
- ✓ Archivos de sistema.
- ✓ Archivos ocultos en el sistema
- ✓ Archivos eliminados que sean recuperables con extracción lógica.
- ✓ Archivos eliminados que sean recuperables con extracción física.
- ✓ Fragmentos archivos de memoria presentes en memoria virtual.
- ✓ Fragmentos de artefactos, de memoria o de red, almacenados temporalmente.

Archivos a encontrarse en una imagen de memoria:

- ✓ Listado de procesos.
- ✓ Procesos en tres estados: activos, terminados y ocultos.
- ✓ Casos de malware, botnets, virus, etc.
- ✓ Archivos abiertos por un proceso.
- ✓ Conexiones de red
- ✓ Credenciales de acceso (nombres de usuario y contraseña o credenciales más complejas como encriptación).
- ✓ Claves en memoria.
- ✓ Claves de encriptación (TrueCrypt, BitLocker o de otro tipo), claves de servicios manejadas por programas, etc.
- ✓ Archivos en memoria por procesos.
- ✓ Usuarios conectados al equipo, local o remotamente.
- ✓ Dispositivos conectados al equipo.
- ✓ Redes a las que tiene acceso el equipo.
- ✓ Librerías, DLLs y drivers cargados en el sistema

Archivos a encontrarse en un volcado de red se puede recuperar la siguiente información:

- ✓ Actividad del equipo en la red local:
- ✓ Archivos compartidos.
- ✓ Archivos accedidos en otro equipo.

- ✓ Documentos impresos
- ✓ Actividad e historial del equipo en Internet:
- ✓ Archivos que fueron compartidos.
- ✓ URLs y sitios accedidos.
- ✓ DNSs utilizados.
- ✓ Paquetes con datos y aplicación
- ✓ Utilización de VPNs.
- ✓ Accesos remotos a equipos

Archivos a encontrarse en otros dispositivos

- ✓ Listados de llamadas.
- ✓ Mensajes recibidos y enviados.
- ✓ Páginas de internet visitadas.
- ✓ Datos de localización geográfica.
- ✓ Aplicaciones instaladas.

11.2 Anexo 2: Acta de levantamiento de soporte de evidencia digital

ACTA DE LEVANTAMIENTO DE SOPORTE DE EVIDENCIA DIGITAL N°

DATOS DE LA CAUSA	FECHA	HORA DE INICIO		HORA DE FINALIZACIÓN	
	CAUSA N°				
	PROCESADO				
	OFENDIDO				
	JUEZ PONENTE				
	DEPENDENCIA JUDICIAL				
	FISCAL DE LA CAUSA				

DATOS DEL PERITO	INFORMÁTICO		TELEFONÍA		OTROS	
	APELLIDOS Y NOMBRES					
	OBSERVACIONES					

LUGAR DEL LEVANTAMIENTO	COMERCIO		DEPÓSITO		OFICINA		CASA		DEPARTAMENTO	
	CALLE PRINCIPAL						CALLE SECUNDARIA			
	NÚMERO		PISO		DEP.		LOCALIDAD			
	OBSERVACIONES									

DISPOSITIVOS											
LEVANTAMIENTO DE SOPORTE DE	CPU		LAPTOP		MARCA	MODELO		GENERICA			
	CELULAR		TABLET								
	NUMÉRO DE SERIE					ENCENDIDA		APAGADA			
	DISPOSITIVOS CONECTADOS	COPIA RAM	SI	NO		FOTO PANTALLA	SI	NO	N°		
		PEN DRIVE				MAQUINA FOTOS			TELEFONO		
		OTRO									
	OBSERVACIONES										

ANEXO FOTOGRÁFICO

OBSERVACIONES