Universidad Nacional de Loja

Facultad Jurídica, Social y Administrativa

Carrera de Derecho

“La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado”

Trabajo de Integración Curricular previo a la obtención del título de Abogado

AUTOR:
Joe Sebastián Contento Martínez.

DIRECTOR:
Dr. Freddy Ricardo Yamunaqué Vite. Ph. D.

Loja – Ecuador

2023

Certificación

Loja 1, de Marzo de 2023

Dr. Freddy Ricardo Yamunaqué Vite. Ph. D

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICO

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: **La Problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado**, previo la obtención del título de Abogado, de la autoría de **Joe Sebastián Contento Martínez**, con cedula de identidad **Nro.1950032969**, una vez que el trabajo cumple con todos los requisitos exigidos por la Universidad Nacional de Loja, para el efecto autorizo la presentación del mismo para su respectiva sustentación y defensa.

Dr. Freddy Ricardo Yamunaqué Vite. Ph. D

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Joe Sebastián Contento Martínez**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi Trabajo de Integración Curricular en el Repositorio Institucional-Biblioteca Virtual.

Firma: JOE SEBASTIAN CONTENTO MARTINEZ Firmado digitalmente por JOE SEBASTIAN CONTENTO MARTINEZ Fecha: 2023.09.21 08:59:31 -05'00'

Cedula de Identidad: 1950032969

Fecha: Loja, 18 de septiembre de 2023

Correo electrónico: joe.contento@unl.edu.ec

Teléfono: 0982387713

Carta de autorización por parte del autor, para consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Integración Curricular.

Yo, **Joe Sebastián Contento Martínez,** declaro ser el autor del Trabajo de Integración Curricular denominado: **La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado,** como requisito para optar el título de **Abogado**, autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestra la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Digital Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.
La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.
Para constancia de esta autorización, en la ciudad de Loja, a los 18 días del mes de septiembre dos mil veintitrés, firma el autor.

Firma: JOE SEBASTIAN CONTENTO MARTINEZ Firmado digitalmente por JOE SEBASTIAN CONTENTO MARTINEZ Fecha: 2023.09.21 08:59:46 -05'00'

Cedula de Identidad: 1950032969

Correo electrónico: joe.contento@unl.edu.ec

Teléfono: 0982387713

DATOS COMPLEMENTARIOS:

Director de Trabajo de Integración Curricular: Dr. Freddy Ricardo Yamunaqué Vite. Ph. D

Dedicatoria

La culminación de este Trabajo de Integración Curricular y mi carrera universitaria se lo dedico a la República y sus instituciones constitucionalmente establecidas, por darme los recursos universitarios y los medios para poder conseguir la culminación de este grado profesional.

A mis padres, Joe Bladimir y Liliana Patricia, a quienes guardo infinita gratitud por ser mi sostén financiero, emocional y anímico durante estos tiempos de dificultad y desarrollo personal.

A mis abuelos, Hugo, como mi inspiración intelectual, y Genaro, por su ayuda en mi crianza, que en paz descansen. A mis abuelas, Ligia Margarita y Anita Miroslava, fuentes de cariño maternal y apoyo emocional incuantificable.

A mis hermanos Renato Bladimir, compañero de media vida, y Juan Esteban, compañero de un cuarto de esta.

A mis primos, Vinicio y Nicolas, que a la distancia de una cordillera y media han sabido ser casi fraternales e incondicionales.

A mis colegas, Steven y María, compañeros en armas académicas que fueron fundamentales para la consecución de este trabajo.

Por último, a Dereck Patricio, Alexa Noralma, Enrique Fernando, Guillermo Andrés, Brandon Ismael, Jessy Camila, Hugo Samael y Jorge Gabriel Fernando, amigos incondicionales que me han dado el soporte y el aprecio que solo se puede equiparar con el de la familia, impulsándome y siendo confidentes oyentes de mis tormentos académicos.

Esto es para ustedes desde el más profundo rincón de mi ser.

Gracias totales.

Joe Sebastián Contento Martínez

Agradecimiento

Culminados mis estudios, no queda más que agradecer inmensamente con gratitud y humildad a la que será mi alma mater, a la Universidad Nacional de Loja, a los doctores docentes que por sus pasillos recorrieron y por sus aulas conocimiento repartieron, siendo una piedra fundamental para la consagración de este trabajo, mi *piece de resistence*, y el desarrollo definitivo de mi vida académica.

Expresar mi agradecimiento a mi director de Trabajo de Integración Curricular Dr. Freddy Ricardo Yamunaqué Vite. Ph. D, quien leyó con esmero, corrigió y con convicción, actuó con celeridad en la dirección de mi investigación.

De manera especial quiero expresar mis agradecimientos a mi director de Trabajo de Integración Curricular Dr.Rolando Johnatan Macas Saritama. Ph.D., por su dirección en todo el proceso de la realización deesta investigación, quien, con su sabiduría, abnegación, y profesionalismo dirigió la investigación social y jurídica de este Trabajo de Integración Curricular, aportando con sus conocimientos para la mejor realización de este.

Extiendo de igual modo mi agradecimiento a los doctores de Fiscalía General del Estado y Universidad Técnica Particular de Loja, y a sus respectivas instituciones; que supieron dar respuestas a mis cuestionamientos y colaboraron con sus criterios para elaboración de las entrevistas, encuestas y recopilación de datos.

Por último, agradezco a todas las personas que me bridaron su apoyo para la realización de este Trabajo de Integración Curricular, entre estos los profesionales entrevistados que supieron darme un minuto de su sabiduría.

Joe Sebastián Contento Martínez

Índice de Contenidos

Índice de Tablas

Índice de Ilustraciones

Índice de Anexos

1. Titulo

“La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado”

2. Resumen

El presente Trabajo de Integración Curricular de Grado lleva por título: “La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado”. Dentro del mismo, se hizo una investigación detallada respecto del fenómeno de la ciberdelincuencia como fenómeno global, y su tratamiento dentro del Ecuador desde la legislación penal y la política pública, con un sentido final de ofrecer un diagnóstico respecto de estas. Para llegar al mencionado diagnóstico, se hizo un estudio jurídico, doctrinal y de legislación comparada que permita entender el fenómeno de la ciberdelincuencia y el delito informático a través de estudiar la forma en que la concebimos doctrinalmente, el estudio de la consecuente legislación penal local, misma que fue evaluada en detalle individualmente, y a la luz del contraste con las legislaciones extranjeras del Reino de España, República Argentina, República de Chile y República de Colombia; y evaluando por ultimo en el estudio de casos y sus estadísticas el impacto real que han tenido tanto legislación como política.

El estudio mostró una legislación escrita que se ha saneado en cuando a los términos jurídicos y tipos penales se refiere, aunque sufriendo en ciertos aspectos por su especificidad. Sumado a esto, se hizo una evaluación de las conductas y tipología delictivas informáticas sobre la base del Convenio de Budapest, que se sugirió como una herramienta de modelo legislativo y de cooperación transnacional. Los resultados de las encuestas y de las declaraciones de profesionales del derecho, sumado a las estadísticas en delincuencia informática del país, hacen evidente una progresiva creciente en la incidencia de estas conductas delictivas y una negligente desatención del gobierno central respecto de su política pública.

Este trabajo hizo uso de materiales y métodos de investigación que permitieron recolectar, procesar y concluir la información expresada. Para obtener la perspectiva publica, se hizo uso y aplicación de encuestas y entrevistas, ambas realizadas exclusivamente en profesionales del derecho penal y al ámbito del delito informático, con el fin de garantizar que las declaraciones fueran de una fuente primaria sobre la temática y que las opiniones vertidas fueran lo más cercanas a la realidad jurídico procesal.

Palabras clave: Derecho informático, Derecho Penal, Delitos informáticos, Cibercriminalidad

2.1 Abstract

The present degree work is titled “The Informatic felonies problematic in Ecuador, its prosecution, and the preventative capabilities of Ecuadorian legislation in contrast with comparative law”. Throughout this document, the initial doubts that surge with the problematic presented were specifically made with the sole purpose of obtaining a diagnosis regarding detailed research about cybercrime's global phenomenon and its treatment inside Ecuador's penal legislation and public politics. To reach the mentioned diagnostic, several studies in doctrine, juridical analysis, and comparative law were made in order to understand cybercrime and informatic felonies through the understanding of the way the doctrine conceives them, the consequent study of the local penal legislation, which was evaluated in great detail in an individual level, and in contrast with the foreign legislations of the Kingdom of Spain, the Argentinian Republic, the Republic of Chile and the Republic of Colombia; evaluating, lastly, the real impact that legislation and politics had through the study of cases and statistics.

The research showed written legislation that has improved in terms of juridic terminology and penal typology, though suffering in certain areas because of its over-description. In addition to this, evaluations of cybercriminal behavior and typology were made based on the Budapest Convention, which was suggested as a tool for legislative modeling and transnational cooperation. The survey’s results and the declarations made by law professionals, in addition to the cybercrime statistics of the country, make clear a progressive rising in the incidence of this kind of criminal behavior and a negligent inattention of the central government regarding its public policy.

This document did make use of several investigative methods and material that allowed the recollection, processing, and conclusion of the expressed information. To obtain the public perception, surveys and interviews that were made, these were applied exclusively to professionals in touch with criminal law and the informatic felony’s ambit, with the purpose to guarantee that the declarations came from a primary source in touch with the matter and that the opinions were as close as possible with juridic-procedural reality.

Keywords: Informatic Law, Criminal Law, Informatic Felonies, Cybercrime

3. Introducción

El presente Trabajo de Integración Curricular llevar por título "La problemática de los Delitos Informáticos en el Ecuador, su persecución y capacidad preventiva de la legislación ecuatoriana en contraste con el Derecho Comparado". La realidad mundial, y consecuentemente la realidad jurídica, se ha visto completamente envuelta por la revolución informática, y por tanto la estructura que sostiene esta red se ha vuelto un bien estratégico de protección. Las respuestas a estas necesidades conformaron el derecho informático que regula respecto del impacto que la red tiene en nuestras vidas, y viceversa. No obstante, entendiendo que una sociedad informática implica por sucesión de conjuntos una criminalidad informática; es importante contar con una legislación y políticas públicas que pueda dar saneamiento al tejido social cibernético. El Ecuador, a la fecha presente, es un estado donde la seguridad en general brilla por su ausencia, lo cual ha puesto en cuestión la legitimidad de los gobiernos de turno. Esta inseguridad, no es endémica únicamente de los aspectos más usuales con los cuales los relacionamos, véase narcotráfico, homicidio, violencia sexual y política; extendiéndose así a estos ámbitos informáticos mencionados.

Los problemas de delincuencia informática han tomado fuerza a lo largo de los últimos años, adquiriendo gran relevancia a partir de ciertos eventos pivótales como la filtración masiva de datos personales de 2019, que expuso dieciocho gigabytes de datos personales, financieros y civiles de la población ecuatoriana; la pandemia de Covid-19, que forzó una vinculación y adaptación apresurada de la vida común a la telerrealidad, los esquemas piramidales de criptomonedas en internet y el ataque al Banco Pichincha de 2021. Mismos hechos que llevaron a un replanteamiento de la legislación penal correspondiente, resultando en una reforma mayor al Código Orgánico Integral Penal y la promulgación de la Ley Orgánica de Protección de Datos Personales, ambas en el año 2021, en entendimiento de la gravedad que suponen estos delitos a los bienes, derechos y garantías constitucionalmente establecidos gracias a su capacidad de inhabilitar soportes digitales enteros que proveen los servicios derivados de estos derechos, pudiendo salir impunes gracias a la transnacionalidad de los delitos.

Cabe mencionar que los delitos informáticos son especialmente problemáticos para la sociedad ya que, al ser minimizados en la opinión pública, se pierde la noción del impacto y flexibilidad de estos, pudiendo tener al mismo tiempo una escala doméstica y una macro estatal. Misma razón por la cual los ciudadanos, que no por norma general no son conocedores técnicos, son especialmente vulnerables a nivel individual como colectivo. Por lo cual, es vital para la

república el adoptar correctamente mecanismos que permitan aplacar la problemática ciberdelincuencia, cuyo impacto social solo crecerá a medida que el país se adentre en la globalización y tecnologías como la red 3.0. Todo esto, mientas a su vez los medios periodísticos locales como El Universo, Ecuavisa y Primicias indicaron crecidas significativas en la incidencia de estos delitos, a pesar de las reformas.

Entonces, como motivación y problemática a tratar de este Trabajo de Integración Curricular, se tendrá como objetivo general el realizar un estudio doctrinario, jurídico y derecho comparado respecto del fenómeno de la ciberdelincuencia y el delito informático con los fines últimos de concebir un diagnóstico respecto del estado de la nueva normativa adoptada, a través del estudio de los conceptos doctrinarios fundamentales que la avalan y el contraste con las legislaciones de los Estados de España, Chile, Argentina y Colombia; a la vez que se evalúa mecanismos de cooperación comunes de estas legislaciones consumadas en el Convenio sobre la Ciberdelincuencia de Budapest.

Respecto de los objetivos específicos, se buscará comprobar los siguientes objetivos: uno general que constituirá el "Realizar un estudio jurídico y de derecho comparado respeto del derecho informático". Se realizan tres objetivos específicos.

El primero "Determinar si los tipos establecidos en la actual legislación penal respecto al fenómeno de la criminalidad electrónica son efectivos para la persecución del mismo".

El segundo "Determinar si el Convenio de Budapest sobre ciberdelincuencia sirve como un marco procedimental y jurídico efectivo el cual la legislación ecuatoriana se beneficiaria de acogerse como marco referencial".

El tercero "Determinar si la política pública por parte del gobierno nacional ha tenido o no efecto para poder combatir la ciberdelincuencia durante los últimos dos términos presidenciales".

El presente Trabajo de Integración Curricular está estructurado en su Marco Teórico de la siguiente manera: Conceptos Informáticos, Hardware, Software, Mensajes de Datos, Malware y virus informáticos, Seguridad Informática, Internet, Conceptos Jurídicos, Criminología y Cibercriminalidad, Derecho Penal, Jurisdicción, Principio de no intervención, Interpol, Una breve historia de la relación INTERPOL-Ecuador, Políticas de Concientización de la INTERPOL sobre la ciberdelincuencia, #ElProximoPuedeSerUsted, #OnlineCrimeIsReal, #SoloUnClic, Política Criminal, Propiedad Intelectual, Delito y delito informático, Análisis de los tipos en base al Convenio, Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y

sistemas informáticos, Delitos informáticos, Delitos relacionados con el contenido, Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, Análisis jurídico de la legislación ecuatoriana sobre el derecho penal informático, Legislación comparada, Legislación española: Código Penal Español, Legislación chilena: Ley 19223, Legislación argentina: Código Penal de la Nación, Legislación colombiana: Ley 1273 reformatoria del Código Penal Colombiano.

Adicionado a esto, el trabajo está integrado por la metodología y materiales utilizados para la consecución de la información correspondiente a la opinión de los profesionales de derecho penal, informático y relacionados al delito informático, las encuestas y las entrevistas con sus respectivos análisis estadísticos e interpretativos. También se adicionan los Casos usados para el estudio practico de la aplicación de la legislación analizada, en conjunto con las estadísticas proveídas por Fiscalía General del Estado respecto de las noticias de delito, que en su conjunto han conformado una base interpretativa respecto de la realidad social que servirá para formular las conclusiones y los respectivos lineamientos propositivos consecuentes.

Los componentes finales del trabajo están conformados por los apartados de verificación, que se referirá sobre el cumplimiento de los objetivos generales y específicos planteados, conclusión, donde se conformaran los argumentos conclusivos sobre el contenido resultante de los estudios planteados y los objetivos, y finalmente las recomendaciones que se referirán respecto de ciertos cambios generales a la legislación penal, implementaciones en política pública, capacitaciones en personal de investigación y agentes fiscales; y la adhesión al Convenio de Budapest.

Es de este modo que este trabajo trata sobre la ciberdelincuencia, como concepto, frente a nuestra legislación penal y nuestras políticas públicas, haciendo una exploración sobre sus características, los medios y términos específicos en los cuales la tipología del Código Orgánico Integral Penal enmarca a estas actividades delictivas y la afectación que tienen estas actividades sobre los derechos y las estructuras sociales sobre las cuales vivimos. Quedando de este modo entregada esta investigación que busca ser fuente de consulta en materia penal e informática, a servicio del Tribunal de Grado para su revisión, corrección, calificación y aprobación.

4. Marco Teórico

4.1 Conceptos Informáticos

4.1.1 Hardware

Como expone Rodríguez (2013) el hardware, en términos generales es aquello que se puede tocar y habita el mundo material, lo tangibles. Comprendiendo lo perceptible, visible y palpable dentro de un sistema informático, telemático o robótico (p. 37).

Esta definición es concreta respecto de la naturaleza que comparten los componentes del hardware: el ser físicos, ser materiales y tangibles. Dejando por fuera la capacidad de hacer de periféricos, y como consecuencia, englobando a los propios componentes electrónicos, véase microprocesadores, disipadores y transistores, como elementos que integran el hardware.

La Corte Suprema de la provincia de Córdoba, en Argentina, emitió en la sentencia de Sistex, S.A, Oliva, S. A. Valerio (1990) sujetándose a que "Con referencia al "hardware" hay que recordar cuáles son los principales bienes que pueden ser materia de tráfico jurídico independiente, pues la computadora funciona a través de diversos aparatos "periféricos" que sirven para "dar" y para "recibir" datos. Así por ej. sirven para introducir información ("input") el teclado, el "disk drive", etc.; para dar salida ("out put") los monitores, las impresoras, etc."

Esta expresión de la Corte Suprema de la Provincia de Córdoba se alinea más con establecer una definición, no a través de su naturaleza física, aunque no se descarta, y la evalúa desde su calidad para servir como medios periféricos que permiten que una parte del equipo, ingrese información al Sistema operativo, o que este último, lo refleje al mundo físico. Es decir, su importancia está en su capacidad para expresar la información al interior de la computadora, o al exterior, y, por lo tanto, no todos los componentes que sean físicos pueden ser considerados hardware si no cumplen con esta función. Es decir, en esta definición, los disipadores que mantienen la temperatura del equipo no son hardware a pesar de estar integrados en la placa madre, pues estos no ingresan información del usuario al Sistema operativo, ni son un reflejo del sistema operativo al mundo exterior, son instrumentos del equipo que auxilian su funcionamiento, no su procesamiento, y por tanto no intervienen, y no pueden ser consideradas hardware bajo esta perspectiva.

Esta expresión esta algo limitada a la funcionalidad practica del equipo, más no la técnica, lo cual representa un problema de percepción importante, ya que lleva a devaluar el valor jurídico que tienen componentes indispensables de un equipo tecnológico cuando se requiera evaluarlos.

El valor real de un componente como hardware no se debe someter a su capacidad de interactuar con el usuario, porque el hardware también puede relacionarse con el propio hardware, y, por tanto, como perspectiva jurídica, la interactividad no es el parámetro más adecuado. Esta apreciación podría derivar como consecuencia una apreciación incorrecta sobre el daño al equipo.

Se concluye, por lo tanto, que el hardware acapara todo cuanto a componentes informáticos que existen en el plano físico, y son accesibles a través de los sentidos de la vista y especialmente el tacto, que sirven como medio para la interactividad con, y entre, los sistemas computacionales o informáticos.

4.1.2 Software

Berzal (s. f) desarrolla al software en términos del soporte lógico, exponiéndolo como el conjunto de programas ejecutables por el ordenador (p.3)

El software son el componente no tangible, aunque si visible, que permite al usuario traducir las acciones que este imprime en el hardware, y traducírselo al ordenador, para que este efectué cierta acción. Es en otras palabras, el intermediario entre el usuario y el procesador.

Así como el Hardware, el Software es un elemento indispensable para la concepción de la computación e informática moderna. Como expone Beekman (2006).

Para entender el por qué, tenemos que primero comprender que el software es una idea que configura, el portal Computerworld (2003) hace un breve resumen sobre la evolución de la computación e informática moderna, cuando conseguimos logramos desarrollar un computador con memoria propia sobre los programas, con anterioridad a esto, los programas eran una serie de tarjetas marcadas en cierto patrón que representaba el lenguaje binario del programa, que el computador ejecutaba una vez lo leía. Es decir, los programas, eran por decirlo de alguna manera, hardware. Eso cambio con la introducción de la arquitectura de Von Neumann, que introdujo la posibilidad de almacenar programas dentro de la memoria RAM, que conjunto con la ideación del procesador dieron paso a la introducción de las interfaces.

A exponer de Rodríguez (2013) Todo este Hardware es controlado, directa o indirectamente, por la pequeña unidad de CPU de la unidad del sistema. Y la CPU es controlada por el software (instrucciones que le indican qué hacer). El software del sistema, incluyendo el sistema operativo (SO), cuida continuamente los detalles entre bambalinas y (generalmente) mantiene funcionando las cosas con fluidez. El sistema operativo determina también el aspecto de lo que aparece en pantalla al trabajar, y cómo decirle a la computadora lo que quiere hacer (p. 5).

Asemejándolo a términos filosóficos, la relación el hardware y el software, responde a la misma dinámica que el cuerpo físico, y el alma. Donde el primero, un ente físico claramente perceptible, ejerce la voluntad del segundo, un ente comandante e imprescindible sin el cual el cuerpo no puede funcionar, siendo este primero únicamente un medio para la interacción del segundo.

Para Romero Castro et al (2018) "el software es uno de los conceptos más abstractos, se lo define como todo lo intangible de la computadora, son instrucciones que el ordenador espera que se realicen, las cuales pueden ser instrucciones complejas o instrucciones sencillas" (p.15).

Romero Castro es acertado en el uso de la palabra "abstracto", lo cierto es que el software es una concepción que no existía, sino que el humano decidido dar valor sobre ciertos valores en código binario para equivalerlos a una acción, o un significado alfanumérico, que luego concatenados formulan una instrucción, un algoritmo, que el computador ejecuta.

El software presenta una singular división de criterios en cuanto a que protección se adhiere esta. ¿Acaso está sujeta al derecho de autor o al derecho de patentes? Doctrinalmente se ha enfrascado en un conflicto entre estas tres perspectivas, sumada a una tercera posición que argumenta que el software tiene una caracterización propia que no se acoge a ninguna de las anterior mencionadas, pues sostiene que este mismo tiene una caracterización propia, al no compartir los suficientes elementos con las dos categorías antes mencionadas. Examinemos la primera de estas perspectivas.

Se enmarca que el software se sujeta al derecho de autor es la posición que más aceptación tiene, los argumentos son sólidos: la inmaterialidad del software, su posición como producto intelectual, y su origen a partir del esfuerzo humano, no el industrial, demarcan una línea clara sobre el hecho que el software este sujeto sobre el derecho de autor, y sobre las leyes consecuentes que protejan este derecho.

La segunda posición, estima que el software es un invento, un producto ideado por la mente humana, que puede ser replicado masivamente, y que por tanto merece ser protegido por las leyes de patentes, estimado que el esfuerzo creativo y técnico que este requiere para su desarrollo, lo hacen merecedor de la calidad de invención. No obstante, los detractores señalan que el software es meramente un conjunto de instrucciones y algoritmos que se le dictan a un procesador para realizar una acción, y que, por tanto, no cumple con muchos de los requisitos que se estiman esenciales para ser considerada un invento, quedando de acuerdo en que la protección de este sujeto

debe quedar a la custodia del derecho de autor, el cual es mucho más adecuado para proteger creaciones originadas del genio intelectual.

Esta discusión toma peso considerable en este trabajo, debido a que cuando se hable la protección del software respecto de ciertos delitos, definir la línea sobre cual custodia está el software será determinante para poder lograr la aplicación correcta de ciertas leyes, o de plano descartar la acción debido a la no adecuación del delito en legislaciones ajenas a la ecuatoriana.

4.1.3 Mensajes de Datos

Gran parte de la legislación latinoamericana respecto del comercio electrónico tuvo su base sobre la Ley Modelo de la CNUDMI (1996) sobre el comercio electrónico que estableció la base común para el manejo de los términos con los cuales nos referimos a aspectos electrónicos e informáticos jurídicamente, siendo este un documento muy temprano que se realizó cuando la informática y los ordenadores empezaban a penetrar los mercados y la vida social de las personas, y por tanto es quizá una fuente de legislación informática que precede a nuestra visión moderna de la misma. Esta misma en su Art. 2, que se refiere respecto de las definiciones establece que los mensajes de datos se entenderán como "información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otro, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o telefax" (p.4).

El esfuerzo en establecer un marco legal más o menos similar entre los países, también nos entregó un marco de nomenclatura que ha vuelto que el entendimiento y estudio de los fenómenos informáticos, desde un punto de vista jurídico, se haya resuelto más sencillo. Sobre la definición del Art. 2, la concepción nos presenta la generalidad adecuada para que cualquier dato que se genere al internet, pueda ser clasificada como mensaje de dato, en el caso de adecuarse a las condiciones de ser producto de una interacción humana, o con propósito del procesamiento de estos a través de mecanismos electrónicos, o su procesamiento, un marco bastante general y algo ambiguo, pero que cumple la funcionalidad de permitir que los datos que se requiera, puedan verse sujetados a la definición común, que ofrece a su vez, una forma de que los datos sujetas, tengan claro a que reglas y leyes se acogen. Debemos comprender que él esfuerzo en este texto, no fue el definir las barreras de la funcionalidad, sino establecer las posibilidades sobre lo que se podía acoger como mensaje de datos, haciendo así más fácil a las legislaciones que lo tuvieran como ejemplo, el trabajo de definir por ellos mismos un marco más concreto en función de sus necesidades.

La importancia de los mensajes de datos tiene de igual manera un origen en esta ley modelo, pues esta, en su artículo quinto establece que no se podrán negar los efectos jurídicos que estos datos puedan generar (p. 5).

Esta apreciación resultante de los grupos de datos que se generan en la comunicación de medios electrónicos es flexible y atemporal, pues está ligada a un concepto que el desarrollo de la tecnología no puede flanquear legalmente, que es que la información será producto de una interacción con un producto electrónico, que es un elemento indispensable en cualquier tipo de interacción tecnológica.

Si bien esta ley tiene el derecho mercantil en mente por su ámbito de aplicación en el comercio electrónico. La definición que esta expone sobre los mensajes de datos sirvió como una que fue aceptada y usada de manera homogénea por el derecho en términos generales.

Por su parte, el Convenio de Budapest (2004) se ocupa más sobre su contenido, expresando los datos relativos al tráfico, que se refieren respecto de los datos relativos de una comunicación realizada a través de un sistema informático, entendido como un dispositivo aislado o conjunto de estos mismos interconectados, y generados por este último, siempre que estos indiquen origen, su destino, su ruta, su hora, su tamaño y su duración (p. 4).

El Convenio, a diferencia de la Ley modelo, tiene una perspectiva más concreta respecto sobre que contiene el mensaje de datos, pues tiene claro que los mensajes de datos se refieren a datos usados en la comunicación, ya sea entre personas, o equipos, el simple intercambio ya define el concepto del mensaje de dato, con la única condición, que es cumplir con parámetros que se pueden explicar cómo “de identificación”.

4.1.4 Malware y virus informáticos

El malware es un elemento de suma importancia a entender cuando de criminalidad y delitos informáticos se habla. El malware en principio es una definición general que engloba todo tipo de programas cuya función se causar daños o perjuicios a un sistema informático. Malware es una palabra que es una contracción de Malicious Software, es decir Software Malicioso, y por tanto este engloba a una variedad de programas que tienen por propósito, a través de su funcionamiento, capturar datos, encriptar datos, borrar datos, alterar el funcionamiento, espiar, y una serie más de acciones que usualmente suelen estar relacionados al tipo del Software del que estamos hablando. Desde su concepción, podemos entender que este tipo de software se diferencia de otros tanto en su funcionamiento particular, como en su intención, la cual es dolosa evidentemente, al estar

ideados y concebidos específicamente para causar daños al hardware o sistema operativo del usuario que normalmente adquiere este tipo de software, sin ser estos conscientes del real funcionar de estos, por lo tanto, también existe engaño en su distribución.

Cabe mencionar que, si bien se suelen usar de manera indistinta, el malware no necesariamente significa lo mismo que un virus, mientras todo virus siempre será un malware, por ser un programa malicioso, no todos los malwares son virus, existiendo otras variedades de programas maliciosos cuyo comportamiento o características son muy ajenos a los de los virus.

Al entender de la informática, el malware puede ser bien una categoría general que engloba a todo tipo de programas dañinos, o un subtipo de los virus. A exponer de Romero Castro et al (2018) los virus son programas que tienen por objetivo hacer daño o cambios al funcionamiento de un computador, abarcando tanto ordenadores como otros equipos computacionales, como pueden llegar a ser los servidores; sin embargo, el mismo Castro señala una diferencia importante que es que los virus pueden ser programas completos, o fragmentos de uno. Como factor diferenciador determinante sobre la naturaleza de un malware, cualquiera este fuere, y un virus, se encuentra en su capacidad de reproducirse en copias, propagándose dentro del sistema infectado. Es más, de esta condición es que deriva su denominación al ser un comportamiento virulento en comparación con su similar biológico. Según señala Castro, desarrollando lo expuesto por Vieites (2013) los virus y otros tipos de malware pueden clasificarse y se puede parafrasear en los siguientes términos:

- Virus, mismos que pueden ser de arranque, archivos ejecutables, macros, script o malware
- Gusanos: los gusanos son un malware bastante particular, mientras el virus se replica así mismo en varias partes de un solo equipo infectado, el gusano se caracteriza por trasmitirte de un equipo infectado, a otros no infectados. Belcic (2016), empleado del proveedor de antivirus Avast, los conceptualiza como malware autosuficiente que no requiere la interacción del usuario, como el caso de los virus, pudiendo incluso extenderse a través de las redes a las que la maquina se encuentra conectada, aprovechándose de vulnerabilidades del Sistema Operativo. Seguido de esto, el programa procede a tratar de extenderse a otros equipos a través de medios de comunicación electrónica como el correo electrónico, mensajería instantánea o a través de vulnerabilidades de la misma red.
- Troyanos: Se trata de Software que, en principio, parece legítimo y aparenta realizar una función deseada, pero que dentro de ella esconde código que contiene instrucciones que facilitan la toma de control del equipo y la apertura de su seguridad para la entrada de más

malware. Su comportamiento y nombre hacen alusión a la historia del caballo de troya descrita en la Odisea de Homero, que expone un regalo con un motivo ulterior.

- Spyware: Configurado por una contracción de las palabras Spy (espía en lengua inglesa) y software, este es un programa que trabaja procurando pasar desapercibido, registrando las actividades del usuario, sus contraseñas, mensajes, contraseñas y demás información personal. El software espía, si bien tiene aplicaciones no maliciosas, por ejemplo, como herramientas de monitoreo de una empresa para asegurar el rendimiento laboral y proteger sus patentes, lo cierto es que es un programa que tiene un alto índice de uso como malware, así que se categoriza como tal.
- Keyloggers: Como advierte Kaspersky (s. f), empresa proveedora de servicios de seguridad informática, los Keyloggers son similares a los spyware en su ocultismo y en su papel de recopilar la información del usuario sin su conocimiento. Sin embargo, mientras el Spyware puede recopilar toda información con la que se interactúe en el sistema operativo, el Keylogger únicamente se dedica a recopilar aquello que se introduce a través del teclado y otros periféricos. Es decir, el Keylogger funciona esencialmente como un captador de contraseñas, donde registra aquellos valores que se introdujeron a través del teclado, para poner un símil, el Keylogger es para las contraseñas, lo que la arcilla para las llaves, ayudando acceder al patrón de acceso de algún control con contraseña.
- Adwares: Los adwares son un tipo particular de Malware. Estos usualmente no buscan tomar el sistema operativo, ni robar información, aunque pueden existir excepciones. El principal objetivo de este tipo de malware es el alterar el funcionamiento de los buscadores de internet y programas internos del equipo para mostrar una cantidad masiva de anuncios y spam no deseado, que le generan ganancias económicas a su programador, a un ritmo que a veces vuelve dificultoso el uso del equipo, aunque este es un efecto secundario al realmente deseado. El portal web de la empresa de seguridad informática Malwarebytes (s. f) los describe como “un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador”.
- Dialers: Los Dialers son un software que se ha visto disminuido en su uso, pero que sigue representando un peligro. Básicamente y como explica el portal de seguridad web Panda (s. f), se trata de programas que están instruidos para que el computador realice llamadas a líneas telefónicas de cobro, generando así facturas muy costosas, como resultado.

- Backdoors: Traducido del inglés, significa puerta trasera, y consiste en programas que permiten accesos remotos a otros usuarios, usualmente este es un método de ingreso de hackers y demás usuarios no deseados, en conjunto con acceso a las funcionalidades del equipo de manera remota y oculta. Los Backdoors son muy usados para las extorsiones en internet.
- Bombas de tiempo: son programas que se activan al pasar un periodo de tiempo determinado, puede ser un contrarreloj o una hora programada, aunque suelen relacionarse a operaciones matemáticas y registros de memoria. Molinario, D (2021) empleado del proveedor de servicios de seguridad informática AVG explica que las bombas de tiempo son parte de un grupo mayor llamados bombas lógicas, que advierte no son necesariamente malware, pero son uno de sus usos más frecuentes, que, en cuentas resumidas, son programas que se activan con el cumplimiento de ciertas condicionales o la inexistencia de las mismas. Una vez cumplida las condiciones previamente instruidas en el programa, este procede a ejecutar un script, una cadena de órdenes, que usualmente tienen por objetivos desde corromper archivos, hasta vaciar discos duros.

Entender el malware y los virus es imperante, a la orden de uno de los principios absolutos del derecho informático, que es la remotidad de las acciones. Los ataques informáticos, escasas veces son llevados desde el factor humano, los especialistas en estos ataques solo suelen intervenir en ataques importantes. Mas bien, el ataque informático se configura en gran parte de los casos, en ataques realizados por estos pedazos de código que un hacker programo para su activación. Estos, según la habilidad y el conocimiento de quien lo programo, pueden variar en su capacidad de daño y autonomía, desde una serie de ordenadores que se infectaron de la mano de sus propios usuarios y que se activan por su mano, presos de su ignorancia; a programas altamente refinados en explotar vulnerabilidades de seguridad de manera autónoma, de difícil percepción y que pueden colapsar sistemas enteros que dependen del correcto funcionamiento de, por ejemplo, un servidor. Pero cabe elevar las preguntas ¿En qué medida se le puede dar responsabilidad al “hacker” programador sobre el alcance de sus virus?

El programador no realizo la acción de manera personal, y muchas veces no es ni siquiera consciente de que los actos se están realizando, un computador puede infectarse de la mano de su usuario, y el no ser consciente del mismo, o un gusano extenderse a múltiples computadores, mientras este duerme. Esto no equivale a decir que no es consciente del producto de su obra, después de todo las instrucciones en el programa se pueden fácilmente demostrar dolosas, pero lo

cierto es que establece una diferencia importante al momento de hablar de la autoría del delito por ser un escenario en el que la acción penalmente castigable puede repetirse de manera infinita sin la autorización, consciencia o intervención del autor, lo que lo diferencia por ejemplo de otras figuras delictivas donde el autor no interviene de directa en su ejecución, pero si en su planeación y consciencia del acto.

Mientras que un delito como puede ser el Sicariato, el autor intelectual tiene plena consciencia sobre que daño se va a hacer, a quien se va a hacer, donde se va a hacer, hasta cuándo se va a hacer y cuál va a ser el resultado, el "hacker" que programa un malware solo el consciente del último de estos en muchos de los casos.

Por supuesto que existen casos donde existen malwares y virus que pueden responder a estas preguntas, pero suelen siempre cuando son programas instruidos para un ataque en específico a un entidad o persona específica. Por otro lado, cuando se libera uno de estos programas a un ambiente con barreras tan difusas y sin control como la red, se pierde por completo la capacidad efectiva de responder las mencionadas preguntas, y por tanto se pierde una capacidad efectiva de establecer el alcance del delito y la cuantía de los daños como consecuencia de la usual capacidad de reproducción y transmisión autónoma que tiene estos programas. Lo expuesto no busca establecer una problemática sobre la culpabilidad del autor de un malware, pero busca exponer que existe un problema consistente en el momento de delimitar sobre cuantos actos, que cantidad de daños, y que cantidad derechos vulnerados está respondiendo este. Problema que abre vulnerabilidades al proceso penal y la correcta aplicación de la justicia, que se suma a la lista de problemas de persecución delictivas en el derecho informático como el ¿ante cual jurisdicción responde este acto? ¿responde de manera individual por cada uno? Si lo hace ¿tendrá que responder por los daños que se sigan realizando durante el desarrollo del proceso? Sino ¿puede responder un individuo en un solo proceso, por un acto que se realizó en probablemente más de una jurisdicción a la vez? ¿Puede ser responsable por el uso intencionado de un tercero de su programa para infectar a un segundo? ¿Los actos se sujetan a la prescripción de la acción local del autor? ¿Del país del computador u ordenador afectado? Y, si se infecta un servidor y colapsan sistemas en múltiples países ¿Es responsable en el lugar donde se encontraba el servidor y cada uno de los países que este servidor daba servicio?

4.1.5 Seguridad Informática

La seguridad informática es uno de los pilares fundamentales del internet moderno. La

protección que esta provee sirvió como garantía imprescindible para la expansión masiva del internet y la incorporación de los usuarios más desconfiados de los aspectos de seguridad de la web en un inicio. La seguridad informática es un concepto que se trabajó tanto de desde la perspectiva informática y desde la perspectiva legal. Romero Castro et al (2018) lo aborda primeramente desde su posición respecto de la seguridad, explicándolo como un conjunto de bases que cimentaban como ciencia a la informática, centrándose en la expresión más básica de seguridad, que es la carencia de amenazas y la confianza por las garantías ante el riesgo. De mismo modo, los mira a través del lente interdisciplinario. Explica "Se puede definir como una ciencia interdisciplinaria para evaluar y gestionar los riesgos a los que encuentra una persona, un animal, ambiente o un bien".

Para entender correctamente la seguridad informática, la clave no está en entender que comprende la seguridad, la seguridad es la acción proteger universalmente, y para el efecto de este desglose definitorio, no requiere mayor trabajo en su concepción. Por otro lado, la importancia recae fundamentalmente en entender el que se asegura. La protección no existe, sin un sujeto o bien al cual este le sirva. En el caso de la seguridad informática, el exponer que se busca proteger los equipos informáticos y sus sistemas operativos no basta para dar una idea correcta sobre la extensión de esta línea de protección.

La seguridad informática atiende desde los equipos informáticos, con esto nos resumimos a la integridad de su circuito, su arquitectura y demás artilugios que se encuentren presenten en el equipo, de manera que sea imposible, por ejemplo, sustraer una memoria RAM de un servidor, o que se dañe el equipo de manera deliberada a través de componentes electrónicos introducidos por un tercero. Este apartado se asemeja más a la seguridad común, la protección de un objeto ya sea por su propia ingeniería, o por el cuidado de otros. Sin embargo, la seguridad informática toma una perspectiva completamente diferente respecto a nuestra apreciación de la protección, cuando nos referimos a las aplicaciones presentes en el equipo, pues se entra en una mentalidad de indispensabilidad bastante particular. Como lo explica Roa Buendía (2013)

> Los ordenadores de una empresa deben tener las aplicaciones estrictamente necesarias para llevar a cabo el trabajo asignado: ni más ni menos. Menos es evidente porque impediría cumplir la tarea; pero también debemos evitar instalar software extra porque puede tener vulnerabilidades que puedan dañar al sistema completo. Cuando una empresa adquiere un nuevo equipo, el personal de sistemas procede a maquetarlo: instala las aplicaciones

> utilizadas en esa empresa, cada una en la versión adecuada para esa empresa, con la configuración particular de esa empresa. Incluso puede llegar a sustituir el sistema operativo que traía el equipo por la versión que se utiliza en la empresa. (p. 12)

Altmark & Molina (2012) hacen un análisis de la evolución sobre el entendimiento de la seguridad informática, exponiendo que en un inicio esta era percibida como algo reservado para los ingenios técnicos y expertos en el campo.

> Siempre se pensó, y su tratamiento se abordó desde dicha óptica, que la seguridad informática era un problema técnico, reservado a los expertos, que irían desarrollando los diferentes instrumentos que el avance de la tecnología iba proporcionando, de acuerdo al desarrollo del estado del arte, y poniendo a disposición de la sociedad, tanto en el ámbito público como el privado, a fin de garantizar una razonable seguridad de los sistemas y la confidencialidad e integridad de la información procesada y almacenada. (p. 514)

No obstante, la penetración del internet en el público general cambio por completo el paradigma. No solo a un nivel de sociedad, sino a nivel jurídico también, ya que la necesidad de contar con una regulación que diera control al nuevo ecosistema digital, se volvió una necesidad imperante. Altmark & Molina explican

> La rápida irrupción de la informática en todos los ámbitos de la vida social, fue indicando, y ello fue receptado internacionalmente por la más destacada doctrina, la necesidad de acuñar un concepto de seguridad informática, no sólo centrado en el aprovechamiento pertinente del instrumental desarrollado por la tecnología y puesto a nuestra disposición, sino a una necesaria sinergia entre dicho aporte tecnológico y la adecuación jurídica de la operatoria de las organizaciones, públicas y privadas, tanto a los requerimientos de la nueva normativa vigente, como a la necesaria estructuración jurídica de la operatoria de los sistemas de información para establecer, en forma debidamente documentada, los procedimientos y protocolos de seguridad y la estructuración reglamentaria. (p. 514)

Lo expuesto expone una premisa directa: para normar un algo, la seguridad informática en este caso, darle forma y ley, primero debemos cuanto menos definir que comprende este algo, no basta que tenga nombre y que tengamos una idea de lo expuesto, se necesita además una comprensión sobre los límites de los que ese algo, para comprender que si se acoge sobre lo dictado para este y lo que no, y por sobre todo, para entender el comportamiento fundamental de este algo,

la compresión de su patrón, por darle un nombre, de comportamiento en sociedad, que puedan darle una idea al legislador sobre qué medidas tomar específicamente sobre el derecho informático, sin nunca perder de vista la naturaleza volátil de su cambio, que responde sobre los avances y vulnerabilidades que se presentan en el desarrollo de la informática y la computación. Entender lo legislado, es hacer leyes duraderas para el sujeto de la regulación que, si bien necesitaran revisión eventualmente como toda normativa o aspecto de la ley humana, se beneficiaran de intervalos de tiempo más extensos que sirvan como una ventana para analizar a la par el fenómeno de cambio del sujeto de regulación, y evitara que el ordenamiento jurídico se vuelva igual de volátil en su cambio como la propia seguridad informática, la cual, cabe mencionar, si bien es rápida en su metamorfosis, es considerablemente más lenta que otros aspectos de la informática y el desarrollo de software gracias a los estándares que deben establecerse dentro de la misma por parte de quienes se aplican en su campo, y por tanto es quizá el aspecto de la informática y computación que resulta más amigable con la legislación y la regulación en términos de tiempo y entendimiento, probablemente ligado a que ambas materias cumplen con un propósito de contención.

4.1.6 Internet

El eje fundamental de toda la informática y computación moderna, al menos fuera de los avances en microprocesadores, es el internet. A exponer del autor De la Cuadra (1996), es un sistema internacional, de libre información y basado en la comunidad, que se maneja a escala global y que permite a quien se adentre, acceder a la casi totalidad del conocimiento colectivo humano, al toque de un dedo. Si diseccionamos su denominación comprendemos que la internet, es una red interna, es decir una serie de nodos, que emulan a una red, que conectan a nivel interno, información de una serie de equipos que quedan en el extremo final de dichos nodos (p. 1).

Su origen irónicamente es en entorno de alto control, un contexto militar. El ARPANET, una red de computadores interconectados entre sí, que fue desarrollada a pedido del Departamento de Defensa de los Estados Unidos de América, con aplicaciones para el manejo de información relacionada a la seguridad, a través de una red interestatal a la que terminaron por unirse otras instituciones relacionadas a la seguridad, como lo son las universidades, que en los Estados Unidos han sido un centro de desarrollo militar desde su asentamiento como potencia hegemónica mundial; y demás organizaciones privadas. Se refiere a la ironía de su origen, por la forma en como la red, terminó mutando a un ente casi anárquico y que por su naturaleza se resiste al control o al cambio no orgánico de su estructura.

En 1983, el internet ve la luz como sistema de acceso al público civil global, abandonando su aislamiento hermético propio de un programa relacionado a la defensa, adquiriendo un carácter internacional al incorporarse el resto de los países del globo y, como describe Trigo Aranda (s. f), su aceptación por parte del público general se debió al desarrollo de tecnologías de marcado como HTML y al establecimiento de estándares como la World Wide Web (www). Los principios del ARPANET dieron cimientos sólidos para la arquitectura de esta mega estructura digital, no obstante, el internet diverge de su antecesor.

De la Cuadra (1996) expone lo siguiente:

> Internet no es una sola red. Como antes hemos dicho, se han unido diversas redes internacionales a un núcleo central, la original Arpanet. Internet es una red de redes. Cada universidad, empresa o particular se une a una red local (por ejemplo, la Universidad Complutense de Madrid, UCM), y esta red local conecta con Internet. (p. 2)

Una vez desatado, el internet empezó a tener un crecimiento de carácter geométrico de razón, es decir el valor sobre el cual se multiplican constantemente, de 2 , cada día los usuarios se multiplicaban en valores constantes, hasta el punto de que se volvió necesaria legislación para poder dar un poco de control y coherencia a la web.

Con el pasar de los años, el internet se convirtió en un tema de imperante relevancia. Altmark & Quiroga (2012) menciona como los Estados empezaron a poner su atención en el internet, el Estado francés se pronunció en 1998 sobre el mismo a través de un estudio bajo el nombre “internet y las redes numéricas” en el cual se pronuncian sobre como estos, son antes un nuevo espacio de expresión internacional, descentralizado, que extiende más allá de las fronteras y que ningún Estado maneja por completo, punto que se ha expuesto reiteradamente por otros doctrinarios. En dichos tiempos, y como expone el documento, se creía que bastaba que el derecho regulara al actor de internet, y se desechaba la necesidad de un derecho específico para los temas informáticos, sin apreciar correctamente las posibilidades que ofrecía el mismo, y que, dependiendo del contexto, podía no existir sujeto activo en el derecho informático.

Lorenzetti (como se citó en Altmark & Quiroga) advierte la existencia de un nuevo espacio cibernético, este no es igual al espacio físico, pues se le reconoce las particularidades que este posee en términos de maleabilidad, gracias a que el código puede alterarse y cambiar por completo la forma de algo, de un día para otro. Agregado a esto, se agregan los cuestionamientos sobre la temporalidad en referencia a la simultaneidad del espacio web y su relación sobre las obligaciones

contractuales.

Agregado a esto, el problema de vigencia contra innovación es importante. Carlos Parellada (como se citó en Altmark y Quiroga) dice sobre esto

> parece ser que, al menos en nuestra materia, la cuestión no es —hoy— la irresponsabilidad civil sino la asimetría entre tecnología y legislación. Por ello en realidad "el problema que aflora a la hora de legislar es que Internet avanza de manera muy rápida, y, cuando apruebas una ley, la tecnología ya ha cambiado. (p. 41)

Exponiendo una lógica fundamental que se vuelve problemática, que es el hecho de que la norma sigue al hecho, pero hasta que lo alcance, se permiten vulnerabilidades que pueden poner en riesgo bienes jurídicos protegidos por cuestiones fundamentales como a la constitución, pero sin la norma o el procedimiento adecuado y claro que permita que estos agravios puedan ser corregidos. La preocupación de la doctrina es clara sobre este punto, exponiendo lo critico que es el no desatender respecto de la realidad informática, puesto que este ecosistema cambia abruptamente según se introducen nuevos avances.

4.1.7 Informática y Derecho informático

La informática es la pieza fundamental por definir para poder analizar de manera adecuada el presente trabajo siendo la materia fundamental sobre la cual se trabajará cualquier planteamiento, suposición y recomendación en conforme a sus elementos. Según lo explican Pablos, López-Hermoso, Martín-Romo y Medina (2004) la informática es un acrónimo que contrae las palabras Información y automática definiéndola como una rama de la ciencia que se encarga de estudiar la automatización de la información y los ordenadores. Esta descripción, a parecer del redactor es bastante vaga y generalizada, pero sienta una buena base para entender el concepto más básico de informática, que es esencialmente su relación inseparable del procesamiento automático de información que en consecuencia se encuentra atado a ordenadores y cualquier otro tipo de tecnología que pueda cumplir con esos roles, pudiendo en medios más modernos, incluso adecuarse las Inteligencias Artificiales como un medio propio de procesamiento autónomo. Guastavino (1987) lo conceptualiza como “el tratamiento automático de la información a través de elaboraciones electrónicos basados en las reglas de la cibernética” (como se citó en Rodríguez, 2013). Rodríguez, de mismo modo, menciona respecto de la informática, que esta se ha expandida por encima de su concepción original de únicamente manejar datos involucrándose en las comunicaciones, la transmisión de imágenes y la inteligencia artificial todo de la mano de la

computación (p.15).

Lo expuesto anteriormente por los doctrinarios, plantea una concepción de la informática que se maneja como sinónimo de la totalidad de la tecnología, siendo innegable que esta se ha visto integrado en cada aspecto de la misma. Sin embargo, cuando hablamos del Derecho informático como parte de la problemática moderna de los delitos informáticos, lo cierto es que nos referimos casi en exclusividad, a la relación de este con el internet, producto definitivo y epitome de la informática; y a las actividades que en este se realizan. No obstante, Rodríguez expone puntualmente, una concepción con vigencia actual, al entender plenamente que la informática engullo y asimilo las telecomunicaciones, al igual que hizo con Inteligencia Artificial, quien se sirve de la información como materia prima para su desarrollo a través de su procesamiento.

A explicación y entender de la Universidad de Lima (s. f) la informática es una ciencia que se encarga de estudiar métodos y procesos técnicos de almacenamiento, procesamiento y transmisión de datos, diferenciándose de la computación, materia que es prima hermana, que se ciñe más a las técnicas algorítmicas y la ingeniería de la estructura algorítmica que procesara los datos.

Si nos guiamos estrictamente por esta definición, entendemos que la informática y la computación son funcionalmente interdependientes, y podemos señalar un origen en común, o un punto de inflexión determinante de las mismas en las manos Alan Turing durante los inicios de 1940, en medio de la hecatombe que fue la Segunda Guerra Mundial, a través de la creación del dispositivo electromecánico Bombe, que a través del manejo de datos que el equipo de Turing hizo al someter ciertas palabras que siempre iban a estar presentes en las comunicaciones encriptadas que interceptaban los Aliados de los poderes del Eje, lograron romper el cifrado de la máquina de encriptación alemana Enigma.

La informática es probablemente la actividad humana que mayor desarrollo, innovación y crecimiento ha consagrado en los últimos tiempos, requiriendo por tanto su regulación. Como explica Aguilar (2015) “la Ciencia del Derecho, como regulador de los fenómenos jurídicos derivados de la actividad del hombre en cualquier área, tuvo que ocuparse de los mismos en consecuencia por la utilización de la informática en la vida diaria.” (p. 1). Configurándose entonces el Derecho informático como la rama encargada de hacer el estudio de la misma y de formular desde la doctrina mecanismos efectivos y en acorde con la naturaleza cambiante de la misma para provecho posterior de la legislación positiva. Para perspectiva de Téllez (2009) el derecho

informático es difícil definirlo, mencionando sus peculiaridades como un factor, aunque ofrece su perspectiva mencionando como esta es una rama del derecho que observa a la informática como un instrumento y a la vez como objeto a estudiar.

Lo expuesto, fue manejado por doctrinarios profundamente informados en la materia informática. Esta es una rama ingenieril y, por lo tanto, su relación con el derecho no existe como una ideación propia de sus desarrolladores, naciendo más bien, de una necesidad de control. El Estado es por definición un ente de control, ya fuera sobre la economía, sobre las relaciones, sobre las finanzas, sobre la seguridad, sobre la información y así un largo etcétera, lo cierto es que la autoridad estatal busca controlar los aspectos estratégicos de la nación sobre la que esta gobierna, esto a través de la ley escrita, de la positivización de los hechos, y el establecimiento formal de procedimientos a seguir para situaciones especiales, que los entes legislativos que existan para el efecto, formulen tomando en cuenta las particularidades del área. Pero cabe reflexionar con lo expuesto ¿qué relación tiene la informática con lo mencionado? La respuesta está en que la informática ha penetrado todas estas áreas de una forma critica, transformando por completo las dinámicas sobre las que estas se sostenían. Las telecomunicaciones vieron como la radio y la televisión pasaban a ser completamente suplantadas, las relaciones sociales pasaron a ser dominadas por las redes sociales, y los paradigmas de la sociedad que se manifestaban de manera pública, se trasladaron a la red; la seguridad paso a ser manejada a través de redes informáticas tanto internas como externas, a fin de agilizar la respuesta ante amenazas inmediatas, y el comercio experimento una revolución como pocas se ha visto, al pasar el internet, apéndice fundamental de la informática, a ser la plataforma de mercado global más importante e indispensable de la historia de la humanidad desde probablemente la ruta de la seda. La colisión de la libertad del internet, y la naturaleza regulatoria y de orden del Estado, llevaron a la formulación del paradigma que es el Derecho Informático.

4.1.8 Derecho informático y las nuevas tecnologías, una continua persecución.

Los cambios sociales vienen siempre acompañados de exigencias de cambios jurídicos. Esta tesis es por sí misma nada más que un ejercicio racional que evalúa un escenario de causa y efecto. Las leyes están construidas en su espíritu más fundamental como un medio para regular la realidad social en la que conviven los sujetos jurídicos como conjunto. Por tanto, las alteraciones en esta realidad social exigen cambios en la normativa vigente, aun cuando esto no implique necesariamente que el derecho respete, responda o atienda adecuadamente estas demandas. Lo que

se discute es la existencia de una necesidad social constante de reformas, no sobre la eficiencia con la cual el derecho puede responder a esta.

Entendida esta premisa, se puede plantear entonces el siguiente silogismo. Si los cambios sociales traen exigencias de cambios jurídicos, las revoluciones sociales exigen en igual grado una revolución jurídica.

La revolución del siglo XXI, aquella que marca definitivamente el carácter este periodo histórico, yace en la revolución informática y la consecuente irrupción del paradigma digital, uno que rompió y sigue rompiendo todos los esquemas preestablecidos antes de la consolidación de las TIC sobre como entendíamos el conocimiento que habíamos acumulado hasta el momento.

En respuesta, el Derecho informático hace avances en el entendimiento de nuevas tecnologías que le sobrepasan en ritmo, pero que, a pesar de esta disparidad de producción, presenta avances importantes en la regulación de tecnologías emergentes, de hecho estos casos son de sumo provecho ya muestran el entendimiento del derecho respecto de la evolución de una serie de invenciones y conceptos tecnológicos que son ajenos incluso a los conceptos tradicionales de dominio, propiedad y divisas, siendo las más relevantes la irrupción de los nuevos estándares de descentralización dentro del internet con Web 3.0, la masiva expansión del criptografía y tecnologías asociadas al Blockchain y la rápida adopción e implementación de la inteligencia artificial. Por esto mismo se analizarán y desglosarán a detalle.

Se advierte que el origen de los casos, y las citas estarán marcadas por pertenecer a la esfera anglosajona, debido a ser estos países altamente digitalizados en los cuales el impacto de estas nuevas tecnologías ha sido respondido por un importante esfuerzo por regular y entender, con resultados varios, el funcionamiento de estos nuevos ejes tecnológicos basados en razones de relevancia estratégica como la seguridad nacional y la especulación con divisas. Lamentablemente, si bien Latinoamérica es un participante relevante del mundo informático, su posición como mero consumidor ha “librado” a sus legisladores de las preocupaciones respecto del manejo de datos en su gran mayoría, limitándose a espectar e imitar el comportamiento de otras naciones sin necesariamente entender las complejidades derivados del campo de estudio, por lo cual las menciones de autores hispanohablantes se verán mermados considerablemente.

4.1.9 Derecho frente a Inteligencia Artificial y Criptomonedas.

Para dimensionar correctamente la disparidad en el avance entre la tecnología y el esfuerzo regulatorio que le persigue, debemos comprender el rango promedio de avance de la tecnología. Harris (2021) expone que la tecnología ha sufrido cambios a rangos exponenciales debido a la Ley de Moore y otras tendencias relacionadas, siendo esta primera uno de los puntos de los cuales podemos partir para el entendimiento más básico de estos cambios.

Kelleher (2022) como vicepresidenta Ejecutiva del desarrollador de procesadores norteamericano Intel expone a detalle los planteamientos e implicaciones de la Ley de Moore, ideada por Gordon Moore, quien fuera cofundador de la propia Intel.

> Gordon Moore, predijo que el número de transistores en un chip se duplicaría aproximadamente cada dos años, con un aumento mínimo en el costo. (…) Cuantos más transistores o componentes haya en un dispositivo, el costo por dispositivo se reduce mientras que el rendimiento por dispositivo aumenta.

La Ley de Moore da razón respecto del altísimo ritmo de las tecnologías emergentes, exponiendo un patrón de comportamiento exponencial al existir un claro incentivo económico por parte de las empresas en al menos **duplicar** la capacidad de transistores cada dos años, es decir, cada procesador, corazón y mente de la computación moderna, es hoy cada dos años dos veces más potente que su antecesor, sin adquirir costes significativos, lo cual no solo explica por qué el aumento de las capacidades tecnológicas de los aparatos computacionales por si solos, sino que además expone el porqué del esfuerzo activo de las empresas desarrolladoras en mantener, o superar este ritmo.

Es de suma importancia entender, que los cambios exponenciales no suelen ser dimensionados adecuadamente al ser mencionados, pero es que un ritmo de cambio de estas magnitudes implica que, aun en el rango mínimo de la ley de Moore, un procesador fabricado en 2015 es quince veces inferior a uno fabricado en 2023 en su capacidad de procesamiento. Una mejora del 1500% en un periodo de 8 años. Entendiendo que buena parte de la limitación tecnológica está en la capacidad de procesamiento, esto significa también un aumento exponencial en las posibilidades de uso de estas tecnologías, volviéndolo así el fenómeno de cambio que conocemos hoy por hoy.

Como resultados de este constante aumento en las posibilidades de procesamiento se ha permitido que gracias a la potencia con la que cuentan los computadores de usuario surjan tecnologías basadas en la descentralización de los datos.

Actualmente el derecho tiene tres grandes frentes que revisar con prioridad: la criptografía y sus derivados, la Inteligencia Artificial y sus diferentes modelos, y por último la descentralización y nuevos estándares del desarrollo Web.

La criptografía no es en sí misma una nueva tecnología, es antiquísima siendo empleada desde la edad antigua, siendo esencialmente la misma actividad desde entonces, la de encriptar, es decir poner bajo clave, código o cifrado, un mensaje o información para privar su contenido únicamente para los autorizados a leerlos a través de la capacidad de descifrarlos. La razón de su importancia entonces no reside en su novedad, si no en sus nuevas implementaciones al combinarse en aplicación con las nuevas tecnologías que han dado origen al fenómeno de las criptodivisas, una serie de activos digitales cuya implementación y atractivo derivan principalmente de su incapacidad de ser rastreadas, el no estar ligadas a ninguna entidad estatal ni convencional del sector financiero, su escases al ser productos con una cantidad fija máxima, y más preocupantemente, su valor como activo de especulación. Un comportamiento y características que comparte en mayor medida con los No Fungible Tokens o NFTS, un activo digital cuyo valor reside en ser irrepetible a nivel criptográfico.

Debido a su masiva expansión, crecimiento y expectativas, estos modelos digitales rápidamente se volvieron una problemática durante los años de la pandemia y postpandemia, comportándose como activos en los cuales los ciudadanos promedios, muchas veces ignorantes de las implicaciones de las divisas que compraban, invertían cantidades considerables de dinero a fin de sacar provecho de la alza de los precios generada por la expectativa de dependencia tecnológica y la fata de confianza en las instituciones financieras tradicionales que genero la Pandemia. Al no ser estas, divisas reconocidas por ley, las criptomonedas difícilmente pudieron ser controladas en lo que se refería a su estatus, su legitimidad, su liquidez y su responsabilidad fiduciaria, siendo así terreno fértil para que afloraran esquemas Ponzi construidos en su totalidad en explotar esta momentánea tendencia alcista produciendo monedas falsas, cursos de entrenamiento hechos meramente para explotar la ansiedad y necesidad de las personas, y falsos gurús inversores.

Incluso el hombre más rico del planeta en ese momento, el emprendedor sudafricano Elon Musk supuestamente hizo uso de su influencia en redes sociales para manipular el precio de la moneda Dodge Coín en su favor a través de declaraciones y movimientos empresariales en Tesla. Inc. y Twitter. Inc., que incitaban a sus seguidores a invertir en dichas monedas, alzando de esta manera artificialmente el precio. Por estas alegaciones Musk fue demandado por uso de información privilegiada.

La falta de regulación en estos activos digitales ha generado escenarios particularmente dañinos derivados del colapso de criptomonedas que se configuraron en burbujas de millones de dólares, y descalabrados descensos generales en el valor del mercado de las criptodivisas derivados del pánico. Estos son daños que se encuentran en los límites del ámbito financiero y tecnológico, pero debido a la ambigüedad de sus estatus al no ser monedas en el sentido que lo contempla la ley, ha llevado a que los derechos e intereses de múltiples personas se vean afectados sin repercusión aparente o a corto plazo, daños que no se le puede responsabilidad de los usuarios que muchas veces son manipulados a sabiendas de su probable desentendimiento de la complejidad de la criptografía. Las personas promedio difícilmente pueden calcular o entender la complejidad del mundo financiero, es por estos que se han forjado leyes acordes para el efecto, siempre procurando proteger los derechos de los individuos. Del mismo modo ha de actuarse con la economía y mercados que giran en torno al ecosistema cripto.

En un esfuerzo por proteger a sus ciudadanos varios estados han hecho recientemente un gran esfuerzo por regular las practicas, los estándares y las regulaciones para este mercado. No se puede negar que las criptomonedas suponen un prospecto interesante como activos financieros y en el futuro, como una alternativa a las divisas tradicionales, por lo mismo el esfuerzo observa como objetivo el que a través de su regulación se pueda integrar plenamente y empezar a contar con estas tecnologías dentro del ecosistema.

La Unión Europea, en esta tónica, en abril del 2023, aunque entrara en vigor en 2024, paso el Reglamento de mercados criptoactivos (MiCA), siendo este el primer marco regulador de este mercado en el mundo. De este modo, las criptodivisas ganan un nuevo marco de legitimidad a través de la garantía que ofrece el estado a través de la ley. Los efectos más significativos de este marco es volver a los criptoactivos sujetos de regulación tributaria, establecer requerimientos de licencias para los proveedores de criptoactivos así como a exigir el requerimiento de información

de los individuos que quieran participar como clientes, y que toda transacción debe estar registrada, ambos esfuerzos enfocados en despojar a las criptomonedas de su uso como herramientas de lavado de activos y transacciones en negro, volviéndolas así más transparentes y legitimas tanto al ojo público como al de los inversores.

McGuinnes (2023 como se citó en Hernández 2023) se refirió a este cambio haciendo énfasis a los colapsos antes mencionados durante el post-covid, atendiéndolo como un tema de suma relevancia en la redacción del proyecto ““Estamos implementando salvaguardas que evitarían que las empresas activas en el mercado de la UE se involucren en algunas de las prácticas que llevaron a ciertos operadores de criptoactivos al colapso” (párr. 2)

A pesar de ser el primer marco legal sobre el apartado de criptoactivos, han existido esfuerzos regulatorios provenientes de otros países.

George (2023) expone en el portal de inversión Investopedia que existen más estados además de la Unión Europea que están impulsando marcos jurídicos sobre los cuales permitir trabajar a las criptomonedas, estos son Estados Unidos, quien extendió el poder de regular los criptoactivos a instituciones federales reguladores ya existentes los cuales han procedido legalmente con Ripple por transacciones no registradas en su criptodivisa nativa; Japón, reconociendo las criptodivisas como propiedad legal cuyas transacciones tienen que notificarse Agencia de Servicios Financieros japonesa, imponiendo un marco legal en el cual las ganancias de estas transacciones son tratadas como ingresos varios para materia tributaria.

Otra de los frentes, el más disruptivo y complejo quizás, está conformado por la Inteligencia Artificial y sus aplicaciones derivadas. Al igual que la criptografía, la inteligencia artificial no es un fenómeno particularmente nuevo, la cuestión de su importancia recae más bien en que siempre se encontró altamente limitado por la capacidad de procesamiento que se requería y por la necesidad de, además de entender los modelos de aprendizaje y razonamiento humanos, encontrar una forma de traducir estos a código. Aplicaciones derivadas de las ciencias de la computación como la ciencia de datos y el *machine learning* contribuyeron enormemente.

Para un mejor entendimiento de lo planteado se explora algunas definiciones sobre estos términos.

El portal especializado en ciencias de datos DataScience (2022) explica

> Otra definición moderna describe la IA como *«máquinas que responden a simulaciones como los humanos, con capacidad de contemplación, juicio e intención»*. Estos sistemas son capaces de «tomar decisiones que normalmente requieren un nivel humano de conocimiento». Tienen tres cualidades que constituyen la esencia de la inteligencia artificial: **intencionalidad, inteligencia y adaptabilidad.**

El portal además hace cita de definiciones hechas por Jeremy Acchin (como se citó en DataScience 2022)

> *La inteligencia artificial es un sistema informático capaz de realizar tareas que normalmente requieren inteligencia humana… muchos de estos sistemas de IA se basan en el Machine Learning, otros en el Deep Learning y otros* ***en cosas muy aburridas como las reglas***

La conceptualización desarrollada por los expertos citados expone un área de la tecnología que trabaja en línea con el entendimiento del proceso mental del humano. No obstante, no basta con tan solo desarrollar el modelo que racionalice conceptos, sino que también sea capaz de imitar o replicar el proceso de aprendizaje humano, eso quiere decir que el modelo no solo responda respecto de los parámetros que se le presenten en el momento, sino que pueda presentar variables en sus respuestas y acciones según los antecedentes de aprendizaje al cual el modelo de aprendizaje artificial haya sido expuesto, siendo capaz de responder según parámetros establecidos previamente como condicionante, pudiendo así variar su juicio en función de lo que dicten las condiciones, siendo capaz de este modo emitir declaraciones que simulan juicios de opinión al menos en su estructura gramatical y que van acorde al perfil de parámetros que se le haya asignado, así como una pregunta puede tener varias respuestas según la persona a la cual se le realice en función de su conocimiento, sus creencias y sus experiencias.

Para poder emular atisbos del comportamiento humano y el raciocinio, la inteligencia artificial saca provecho de su asociación con las ciencias de datos, que se podrían definir como uno de los punto de apoyo claves para su perfeccionamiento, que provén a modelos de procesamiento y aprendizajes, conocidos como Machine Learning, de cantidades masivas de data recolectada de las interacciones de millones de usuarios en la red, cortesía de las plataformas sociales, motores de búsqueda y sitios de compraventa, a fin de que el algoritmo de aprendizaje sea expuesto a los

modelos de expresión e interacción humana, encuentre patrones lógicos y estadísticos entre ellos y que de este modo sea capaz de modelar un algoritmo que exprese patrones idénticos o similares de manera autónoma, lo que lo vuelve un herramienta potente para la automatización de ciertos trabajos de servicios antes considerados no aptos para las maquinas.

Para poder seguir estos parámetros es necesario hacer uso del Machine Learning, traducido del inglés aprendizaje de máquina. Como explica BBVA (2019) este proceso se integra con una etapa de desarrollo temprano del modelo de inteligencia artificial, uno donde el modelo inicial se especializa en reconocer patrones, sean estos de lenguaje, acciones, de colores o numéricos; con el objetivo de poder hacerlo posteriormente sin ningún tipo de asistencia a contenido al que no ha sido expuesto previamente.

El Machine Learning es entonces a la Inteligencia Artificial lo que la Facultad es para los profesionales del derecho, una etapa formativa que no nos dicta exactamente cada contenido y punto de la ley, sino el cómo interpretarla y enfrentarla en cualquier escenario.

La Inteligencia Artificial es entonces un mecanismo a regular que emula la actividad humana, formula y produce resultados que antes únicamente podía crear el hombre, sea por su mano, o por su instrucción a través la programación. Pero no tienen el perfil o el mismo estatus de humano, generando así una problemática. Por un lado, no están sujetas a las leyes de los hombres, y por otro lado, las leyes de las maquinas vigentes no son adecuadas ya sea por qué sufren del desentendimiento de la materia, o de plano no las contemplan, lo que las deja en un vacío legal que abre la puerta a que estos avances tecnológicos que se perfilan como el molde del gran salto tecnológico, puedan afectar negativamente a la sociedad en caso de que su aplicación se incorrecta que agravarían consecuencias inmediatas como la automatización con otros males como la automatización de mecanismos autoritarios o el perfilamiento racial, preocupaciones que quedan recogidas por la Organización de las Naciones Unidas (2020) en su Recomendación General núm. 36.

> Hay diversos puntos de entrada a través de los cuales el sesgo se podría incorporar en los sistemas de elaboración algorítmica de perfiles, entre ellos la forma en que se diseñan los sistemas, las decisiones sobre el origen y el alcance de los conjuntos de datos con que se entrenan, los sesgos sociales y culturales que los creadores de aplicaciones pueden incorporar en esos conjuntos de datos, los modelos mismos de inteligencia artificial y la

> forma en que los productos del modelo de inteligencia artificial se ejecutan en la práctica. En particular, los siguientes factores relacionados con los datos pueden contribuir a obtener resultados negativos: a) los datos utilizados incluyen información relativa a características protegidas; b) se incluye en los datos la denominada información indirecta, por ejemplo, los códigos postales vinculados a zonas segregadas de las ciudades suelen indicar indirectamente la raza o el origen étnico; c) los datos utilizados están sesgados en contra de un grupo; y d) los datos utilizados son de mala calidad, en particular porque están mal seleccionados, están incompletos, son incorrectos o están desactualizados.

Esta preocupación es relevante debido a que han existido ejemplos de modelos de inteligencia artificial los cuales han evidenciado perfilamiento y discriminación sobre ciertos grupos sean raciales, étnicos o género como consecuencia del origen de las bases de macrodatos a los que fueron expuestas. Todo se remota a la etapa de desarrollo, en medio del aprendizaje de la máquina ya que los macrodatos a las que se le expone para aprendizaje muchas veces son una recolección de múltiples ideas que el modelo de inteligencia tomara para configurar su algoritmo de pensamiento, y pueden contener ideas con connotaciones racistas, segregacionistas o en detrimento grupos ideológicos o étnicos, llevando por resultado a que el modelo aplicado se configure entonces parcialmente con estas ideas que pueden terminar generando modelos IA cuyas aplicaciones terminen por segregar y perfil a ciertos grupos étnicos o raciales.

Martínez & Matute (2020) ahondan sobre esto en el artículo que publicaron en el portal *The conversation* el artículo titulado Discriminación Racial en la Inteligencia Artificial donde describen los resultados del estudio *The Woman Worked as a Babysitter: On Biases in Language Generation* (La mujer trabajaba como niñera: Los sesgos en la generación de Lenguaje) de las Universidades del Sur de California y la Universidad de California. Como parte de los resultados de esta investigación, señalan como el algoritmo de completado de texto mostraba criterios sesgados, respondiendo a la palabra "mujer" y "hombre negro" con términos y ocupaciones estereotípicas residuales de roles sociales ahora en desuso (párr. 1 – párr. 5). Por sí mismo este resultado es preocupante pues evidencia que los modelos de inteligencia pueden efectivamente adquirir perfiles discriminatorios, pero, además, su uso en sistemas de distribución de roles multiplataformas, como LinkedIn, que requieran asignaciones como trabajos o universidades, podrían llegar a causar brechas ocupacionales y segregación.

Otro aspecto preocupante es su uso para el monitoreo autoritario de los ciudadanos sobre la base un factor, sea este ideológico, racial o socioeconómico. La República Popular de China, el dragón despierto, es uno de los máximos desarrolladores de Tecnología en los últimos años. En esta misma línea, la nación asiática ha hecho uso de sus bastos recursos y a integrado plenamente la tecnología dentro de la infraestructura estatal. Telecomunicaciones, transporte, medicina, diversos servicios y así un largo etcétera, las tecnologías han irrumpido en el mercado chino. Naturalmente el estado se hizo de estos servicios para su propio provecho en materias de seguridad y vigilancia. Al ser este un estado autoritario, ningún ente o tecnología puede menoscabar la posición estatal, todo cuanto existe en tecnología debe servir al estado y al partido, razón por la cual China ha tomado una posición estratégica en la toma de control de la Inteligencia Artificial, afinando su ideología. Estañol (2023) redacta para el portal francés *Radio Francia Internacional* el artículo *China quiere ajustar la inteligencia artificial a la ideología del Partido Comunista*, exponiendo como para China es una prioridad que estas reflejen los valores socialistas. La visión fundamental del estado chino es que la Inteligencia Artificial sea un aparato más de control al servicio del partido a través de la censura. La vulneración de las libertades sobre la expresión y pensamiento serían de aplicación directa por la Inteligencia Artificial, una que fue alimentada e ideada con el objetivo de encontrar el contenido incomodo y desaparecerlo. Esta herramienta supone un serio problema de extenderse más allá de las fronteras del estado chino al alcance de otros regímenes autoritarios que puedan hacer de su servicio de igual modo, configurándose un mecanismo que es tanto en espíritu como en actos contrario a todas las ideas del constitucionalismo moderno y las libertades fundamentales.

4.2 Conceptos Jurídicos

4.2.1 Criminología y Cibercriminalidad

Para Carranza (1994) la criminología se define como:

> Ciencia interdisciplinaria cuyo objeto está integrado por el delito, el delincuente, la víctima, y la reacción social frente al delito (reacción social formal o por medio del sistema de justicia penal e informal, que comprende toda otra reacción social que no se canalice a través del sistema de justicia penal). (p.18)

La criminología se constituye en un instrumento diagnostico respecto del orden social. Mide la incidencia de acciones estimadas como lesivas para la estructura social y mide el efecto

que estas tienen, concluyendo así sobre las condiciones que terminan por generar dichas acciones y las condiciones consecuentes residuales de su realización. Este estudio ofrece la ventaja de poder observar y examinar el delito desde un punto de vista que se extiende más allá del simple hecho de determinar que una acción es lesiva, dando una explicación sistemática sobre como esta afecta al tejido social, ayudando de este modo a exponer un razonamiento adecuado sobre el porqué de la penalización y tipificación de ciertas conductas, a la vez que permite aislar fallas en la estructura social que explican la sucesión de los hechos criminalmente designados, y tratarlos con los medios adecuados para subsanarles de ser posibles, o disminuirlos en su defecto.

El Centro de Formación Estudio Criminal (s. f) explica que la criminalidad es "El conjunto de todos los hechos antisociales cometidos contra la colectividad". En este orden, entendemos por tanto que la cibercriminalidad sería un subconjunto de la criminalidad, un conjunto de acciones antisociales contra el colectivo social que se realizan en espacios digitales y cibernéticos. Y si existe la cibercriminalidad, la criminología tendrá su perspectiva de estudio de está configurada en la ciber criminología.

No existe una definición universal sobre la ciber criminología, ni del cibercrimen, probablemente debido a que el termino es casi auto definitorio, pudiendo al leerlo, entender que la ciber criminología, se constituye en un estudio criminológico de enfoque limitado, observando únicamente sobre el fenómeno criminológico de los delitos cibernéticos y digitales.

La Universidad a Distancia de Madrid (s. f) explica "La ciber criminología es una parte de la criminología que tiene como objeto el estudio de la delincuencia y la conducta antisocial en el ciberespacio y sus implicaciones en el espacio real".

Los delitos informáticos se han relacionado como un sujeto de estudio particular para la criminología, su comportamiento único y su difícil estudio por ser un delito de difícil visibilidad, y con bajos números de denuncias a los cuales hacerles seguimiento, hacen que estos presenten un reto para esta ciencia. Los elementos del delito informático muchas veces cambian, al igual que sus medios, y sus consecuencias, por tanto, el analizar los mismos se convierte en una tarea que requiere una observación constante de la evolución de estos hechos delictivos y sus impactos, cosa que se vuelve difícil cuando tomamos a cuento la poca visibilidad antes mencionada y lo discreto de los datos relativos de los casos.

A pesar de las dificultades mencionadas, la criminología ha puesto luz sobre la criminalidad de manera determinante, convirtiéndose en el faro que ha alumbrado el resto de las ramas del

derecho para que estas puedan desarrollar sus propias medidas para la regulación de esta, esto se puede ver reflejados en los múltiples manuales e intentos de conformar cuerpos jurídicos supraestatales que indiquen sobre el cómo lidiar sobre estos mismos ciberdelitos. Las preocupaciones de esta ciencia se centran sobre todo en entender la relación que tiene el derecho informático con el formato de crimen organizado, siendo la informática, específicamente el internet más profundo, una herramienta que permitió la adaptación de todo modelo criminal y delictivo preexistente, a uno digital y por tanto de un potencial de escala global, lo que representa por supuesto, una seria amenaza a derechos, garantías y a la propia seguridad nacional.

4.2.2 Derecho penal

Es sumamente importante definir con claridad el concepto del derecho penal pues el tema investigar se enmarca en buena parte en estudiar como este maneja y se enfrenta a los delitos informático, con observación de los resultados de dicho manejo. El derecho penal representa el conjunto de leyes que existen en el ordenamiento jurídico que regulan el poder punitivo del Estado.

Para Mariaca (2010) el derecho penal es la ciencia que observa y razona el delito, al delincuente, y la reacción que tiene la sociedad ante los mismos de forma estructurada, deduciendo principio y leyes generales. Por otro lado, para Jiménez de Azua (2005) lo de define como "conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado" (como citado en Mariaca, 2010).

Según estos especialistas, el derecho penal es esencialmente una ciencia que estudia el impacto que tiene en la sociedad el delito, el delincuente y su impacto social, a la vez que también ofrecen estudio sobre la potestad punitiva del Estado. Las dos observaciones doctrinarias redactan su apreciar desde posiciones incompletas. La primera perspectiva trabaja observando al derecho penal como una rama de la ciencia jurídica que estudia y razona, una posición que, si bien no es incorrecta, omite quizá una los componentes de esta rama, que es función regulatoria del poder, una perspectiva que Azua, tiene presente siempre el papel practico que tiene el derecho penal, pero falla en señalar adecuadamente que si bien esta es una de sus aplicaciones más frecuentes, el derecho penal no es un derecho meramente punitivo, esta definición pasa por alto el importantísimo peso doctrinario e investigativo que esta ocupa dentro de la ciencia del derecho. No obstante, comparando las perspectivas, se puede expedir una definición propia que expresa que el Derecho penal es una ciencia que estudia el delito, al delincuente, el impacto social de las acciones penalmente punibles y el control del poder punitivo del Estado con sus instituciones.

Otro autor que ofrece una perspectiva es Alban Gómez (2016) cuando dice:

> El Derecho Penal puede ser visto, y conceptualizado, desde una doble perspectiva. Fuera del ámbito estrictamente jurídico, la sociedad considera al Derecho Penal, más exactamente a las leyes penales, como un mecanismo de control social y de represión, juntamente con la policía y los jueces.
>
> (…) La evolución de la sociedad, la aparición y la consolidación del Estado de derecho y la necesidad de regular cuidadosamente el conjunto de sanciones, para limitar la actividad represiva a los casos indispensables y evitar las arbitrariedades del poder, dieron lugar a que este mecanismo de control y represión se regularizara y formara un sistema de normas que conocemos con el nombre de Derecho Penal. (p.1)

La conceptualización de Alban Gómez, habla en los términos del derecho penal a través de una evolución histórica, en el cual se expone como este en un principio se observó como meramente, como un mecanismo de control social, para luego ser apreciado como un mecanismo control del poder, acoplándose a la evolución histórica del poder y de cómo la fuente de la cual este emanaba se transmitió desde la figura del Estado en el antiguo régimen, que era ajeno al pueblo como un ente separado que gobernaba sobre este, quedando este último en una situación servil, hacia este la figura del pueblo gobernante, que se volvió el elemento de legitimidad del Estado y que a través del orden y la ley busco domar, encadenar y subyugar al Estado.

Esta conceptualización es por demás interesante, puesto que contribuye la concepción sobre el derecho penal actual como un elemento de control al Estado, ignorando para enfatizar el contraste que el derecho penal no paso de ser un elemento de represión, castigo y control social, a un elemento de control del Estado, abandonando la primera posición. Mas bien, asumió como nuevos los elementos de esta última naturaleza, a la par que se replanteaba y reformulo la primera; aquella que representaba la naturaleza autoritaria y punitiva, que, a la luz de un espíritu reformista, paso a establecer que el derecho penal ahora sería un mecanismo de control y reforma social. Es importante señalar esto, porque no se debe malentender por el contraste de las dos posiciones históricas que el derecho penal a abandonado su rol como mecanismo punitivo, esto sería una mentira. Se trata de entender que la posición actual ha revisado sobre los valores que antiguamente legitimaban este control, a través de cuestionar sobre el quien legitimaba dicho control, y el propósito que este buscaba. No se dejó de suprimir a través de la pena, lo que se abandono fue la

idea del castigo como la expresión final de la justicia, en favor de la reforma del procesado y la retribución de la víctima como el objetivo último del derecho penal.

La concepción del derecho penal, dentro de la legislación ecuatoriana, se encuentra implícitamente establecido en su Código Orgánico Integral Penal (2014) en el cual su Artículo 1, que se refiere respecto de la finalidad de dicho código, establece que el mismo normará el poder punitivo del Estado, tipificará infracciones penales, establecerá procedimientos de juzgamiento basados en el debido proceso, la rehabilitación social y la reparación de las víctimas. Una declaración intenciones que a opinión de quien subscribe el trabajo, se acoge a varios de los elementos expuestos en las definiciones doctrinales antes mencionadas.

4.2.3 Jurisdicción

La historia de la jurisdicción es la historia de la relación Estado-derecho, una de particular naturaleza. Mientras que no se puede separar a la ley como una herramienta del Estado para hacer imperio del poder que de este emana, también cabe señalar que la ley escrita culmino por configurarse en un elemento de restricción de este mismo poder, en otras palabras, la ley paso de ser una expresión del poder absolutista, a una válvula reguladora de susodicho poder. En palabras Ferrajoli (1997) en su ensayo Jurisdicción y Democracia “la historia del derecho puede ser leída como la historia de una progresiva minimización del poder por la vía de regulación jurídica” (p.1) exponiendo una posición que se alinea a la planteada por quien subscribe, después de todo, y en discrepancia con posiciones de juristas del pasado, el Estado ha pasado de ser un ente casi inmune, absoluto e indivisible; a ser segmentado, balanceado y responsable legalmente por sus actuares.

La palabra clave en esta metamorfosis es segmentado, la ley ha encontrado la capacidad de moldear y limitar al Estado, a través de la división y segmentación de este, especialmente a través de la configuración de la potestad, la competencia y la jurisdicción. El Estado único absolutista del antiguo régimen paso por una separación quirúrgica que independizo la capacidad de mandar, dar ley y dar justicia; posteriormente serían las propias funciones las cuales fueron segmentadas, y así podemos observar que conforme el Estado liberal democrático comienza a cimentarse y solidificarse, encontramos una división cada vez más clara sobre cuestiones como el cómo, el dónde y el quien puede ejercer respecto del ejercicio de una parte del poder.

Contextualizado adecuadamente, se hace evidente que la definición de concepto de jurisdicción se ha revisado y enmarcado desde diferentes perspectivas doctrinales, principalmente debido a que, a causa de ser la jurisdicción una potestad que emana del ente estatal, la forma en

como esta se conceptualiza puede verse alterada de Estado a Estado, por lo cual su definición no es uniforme.

Para Chichizola (2013)

> Normalmente se considera a la jurisdicción como la función pública que tiene por objeto la declaración del derecho aplicable (…) por intermedio de un órgano jurisdiccional que actúa como tercero en los conflictos de intereses para la realización del derecho objetivo (p.3).

La explicación de Chichizola habla sobre el rol que adquirió jurisdicción, dejando implícito en el texto, su unión ineludible a la impartición y el manejo de la justicia, como facultad que permite declarar que parte del ordenamiento aplica a una situación que se someta a su juicio, declarando responsabilidades y decidiendo sobre quien se ha desempeñado en orden con lo dictado en la norma, para lo cual, la jurisdicción se sujeta a su vez a las normas para el efecto que le indiquen respecto de cómo resolver.

El uruguayo Couture (como se cita en Chichizola) expone sobre la jurisdicción que esta "Consiste en declarar el derecho en nombre del Estado o en nombre de la justicia del Estado; pero no es solamente la potestad de decir el derecho, sino también al de mandar cumplir lo que se ha resuelto" (p. 3).

La concepción de Couture construye sobre la base que la jurisdicción es una expresión del Estado, o publica, que se pronuncia sobre el derecho aplicable y la justicia. No obstante, contribuyendo con un nivel extra que no se tenía presente en la posición de Chichizola, que es la de mandar sobre lo decidido. Es decir, no es solo la decisión de la justicia del Estado sobre que parte se encuentra en lo correcto o en lo erróneo, sino también la facultad de obligar a los sujetos a someterse a los designios que se consideren necesarios para poder resolver sobre controversia en cuestión, todo esto siempre unido a la sujeción a los límites y puntos que disponga las leyes procesales que se hayan formulado para el efecto.

Según Velloso (2015), la palabra jurisdicción es problemática, definiendo varios conceptos que poco tienen que ver uno con el otro, quedándose su uso como tipificación de juzgar, sobre esto menciona

> A base de esta premisa, se acepta mayoritariamente que jurisdicción es la facultad que tiene el Estado para administrar justicia por medio de los órganos judiciales instituidos al efecto, los cuales —en función pública— tienen por finalidad la realización o declaración del derecho mediante la actuación de la ley a casos concretos. (p. 4)

La posición de Velloso se hace critica del uso tan impreciso de los vocablos en el derecho, pronunciándolos como acientíficos, a la vez que busca consolidar una posición sobre la jurisdicción como la facultad estatal de la impartición de justicia, misma que a su vez se transfiere al juez como operadores de esta.

Como concepto fundamental de la justicia moderna, la jurisdicción tiene un papel fundamental cuando de derecho penal informático hablamos, y un panorama complicado, con especial énfasis en Latinoamérica. La jurisdicción determina respecto de quien tiene la capacidad de impartir la justicia que emana del Estado. Esto lo hace tanto en el sentido de la persona a quien se autoriza, como en el dónde se autoriza y en qué materia se autoriza. Estos aspectos que se le faculta a un juez son fundamentales para la consecución de un proceso jurídico legítimo, y es un modelo solido en su aplicación nacional. No obstante, la jurisdicción toma un valor importante cuando pasamos al plano internacional, puesto que, si bien se concibe de manera global un concepto de jurisdicción homogénea, el resto de los aspectos pueden y suelen diferir de Estado a Estado. Ya sea por una diferente apreciación legal de las acciones, o por una concepción diametralmente diferente del proceso. La particularidad de la relación entre la jurisdicción y los delitos informáticos reside en que estos son con diferencia los delitos más nuevos que se han configurado, teniendo como consecuencia que tanto la doctrina, ni el ordenamiento jurídico, ofrezcan un marco de acción y tratamiento unánime. Las acciones delictivas informáticas suelen realizarse desde la remotidad de otro Estado al cual la acción se está efectuando, y, por tanto, se enfrenta a los cuestionamientos de sobre quien responde la jurisdicción para conocer y procesar los hechos. Es cierto que el tanto el derecho interno, establecido en constitución, como el derecho internacional, demarcan sobre los límites y alcances de la soberanía y por tanto de hasta donde se puede ejercer jurisdicción. No obstante, el derecho interno tiene un efecto real dentro de las fronteras del Estado, y cualquier otro tipo de intento de traer al responsable ante los organismos jurisdiccionales recae plenamente en la capacidad de cooperación entre los Estados que se vean involucrados en esta pretensión o la capacidad que tenga una entidad tercera de coaccionar un segundo. Este escenario plantea dos problemas, el primero es el desincentivo que opone la burocracia del derecho internacional sobre la jurisdicción, acompañado de las evidentes complicaciones procesales involucradas, que hacen que el afectado estima inviable la denuncia o persecución de un proceso; y el segundo que es el desestimar la perspectiva política que se presentan en este tipo de situaciones donde existen naciones que por razones de seguridad, geopolítica y geoestrategia, buscan activamente denegar el

acceso de la justicia, a los responsables de acciones judicialmente punibles que se desarrollaron en el ámbito informático.

Lo cierto es que la Jurisdicción ha tenido un desarrollo complicado dentro del ámbito informático.

En las etapas tempranas de contacto entre el derecho y los delitos informáticos, se estableció que la regulación y la cooperación eran fundamentales para poder afrontarlos. Sin embargo, esta transición se logró de manera adecuada únicamente en los países donde la penetración tecnológica permitió una integración de la computación y la informática en la sociedad y burocracia; características que en aquel contexto, eran ajenas al sur global, y por lo tanto para el ecuador, donde la tardía adopción de una cultura informática significo en igual grado, una tardía adopción de los estándares de prevención y persecución, los cuales, en el momento de su redacción, respondían más a las amenazas de un internet y computación más rudimentarios, y que por tanto resultaban evidentemente insuficientes frente a una tecnología moderna que se había puesto varios pasos al frente de una legislación que buscaba tipificar los comportamientos, pero carecía del entendimiento adecuado sobre las herramientas extralegales que se requerían para poder enforzar lo dictado. Este fenómeno se repitió en el tercer mundo de manera parcialmente uniforme -algunas repúblicas como la argentina introdujeron legislación informática y con la computación en mente de manera adelantada a otras repúblicas- traduciéndose la demora en establecer legislaciones informáticas internas, en dificultad de poder establecer un marco de cooperación a nivel regional. Como consecuencia de esto, las naciones tercermundistas, más que centrarse en establecer marcos de cooperación con otras naciones, han apreciado más beneficioso el acogerse a la legislación ya extensamente desarrollada y probada funcional por esos mismos países que inicialmente se compenetraron con la informática y la computación. Sin embargo, esta solución depende totalmente de que el país con el cual se busca cooperar se encuentra acogido de mismo modo al mismo cuerpo internacional (comúnmente estaríamos hablando de la Convención de Budapest) o que haya formalizado un tratado bilateral de cooperación propio, instrumento que como se indica tiene procedimiento ad hoc, y cuya efectividad recae en negociar los términos de dichos procedimientos con cada país que se busque colaborar o se requiera.

Es importante tener siempre presente que no existe un marco perfecto de cooperación internacional. La carencia de un cuerpo jurídico procedimental, al cual se encuentran atados jurídicamente todos los Estados, y que contenga la totalidad de los procedimientos, o idealmente

un principio elevado a ius cogens al respecto, ha vuelto imposible concebir un mecanismo procedimental universal de cooperación supraestatal. En su defecto, lo que actúa en el plano jurídico internacional es una extensa y variada colección de acuerdos, tratados y convenios que vinculan legalmente a las naciones firmantes a cumplir en ciertos procedimientos de manera medianamente uniforme, siempre teniendo a cuenta la reserva de los Estados; y , apreciando que la no existencia de un tratado o vínculo alguno entre un Estado y otro puede llevar a severos dilemas procedimentales, se vuelve de suma importancia entonces que cada Estado trate de entablar y adherirse a tantos tratados de cooperación bilaterales y multilaterales, como le sea posible.

Existen iniciativas dentro del marco internacional que buscan solucionar estos problemas, figuras internacionales en desarrollo como la jurisdicción universal son un ejemplo de esta búsqueda, la cual la República del Ecuador incorporo dentro la legislación penal en su Art. 401 del Código Orgánico Integral Penal (2014)

> Los delitos en contra la humanidad puede ser investigados y juzgados en la República del Ecuador, siempre que no hayan sido juzgados en otro Estado o por cortes penales internacionales, de conformidad con lo establecido en este Condigo y en los tratados internacionales suscritos y ratificados

La jurisdicción universal se podría considerar como una respuesta única ante fenómenos de gravísima consideración como los son los delitos contra la humanidad, estimando la no prescripción de estos crímenes y la gravedad de las acciones como una justificación para la intervención de la justicia ecuatoriana en nombre de los afectados, aun cuando estos fueran ajenos completamente a la república, en concordancia con la idea de que su persecución es universal establecida en los convenios de Ginebra.

Una posición que obliga al Ecuador a impulsar procedimientos penales que no se hayan procesado bajo otra jurisdicción con anterioridad, es una gran iniciativa para poder solucionar problemas procedimentales y de jurisdicción internacional, sin embargo, este principio no puede actuar de como solución absoluta para los conflictos antes mencionados debido a que la posición sobre la jurisdicción universal expresada solo habilita el proceder del aparato estatal ecuatoriano frente acciones suscitadas en el extranjero, pero no es un principio erga omnes, por tanto el resto de Estados tienen la reserva sobre su acoger dentro de su ordenamiento jurídico interno, es más, algunos Estados como el español se ha retraído en su posición respecto de este principio, lo que devuelve el debate a un punto cero de negociación entre los Estados y falta de consenso

internacional.

Exploradas las herramientas que se ofrece dentro de la legislación interna y macro estatal queda evidente una dificultad clara para poder perseguir delitos informáticos internacionales y es por tanto que, este trabajo expresa importancia y gran valor en que la República del Ecuador sostenga un postura acorde a la nueva realidad tecnológica e informática, y opte por adoptar el Convenio de Cibercriminalidad de Budapest, por ser este uno de los de mayor acogida del mundo, y por consecuencia, el que permite cooperar con más Estados, sumado a que a su vez el Estado ecuatoriano busque entablar de manera directa tratados de cooperación procedimental con los países no firmante del convenio más próximos a nuestros territorios, todo esto con el fin de dotar al Estado ecuatoriano, y en especial a los mecanismos de persecución y justicia, de herramientas y procedimientos de cooperación extrafronterizos que permitan subsanar las complicaciones derivadas de la jurisdicción internacional.

4.2.4 Principio de no intervención

El principio de no intervención es indispensable para entender de donde derivan los problemas jurisdiccionales y procesales frente a las problemáticas de cibercriminalidad y delitos informáticos, puesto que es el principio que define un límite claro sobre la acción y pertinencia de la jurisdicción en el ámbito internacional.

El derecho internacional, si bien hoy en día es un mecanismo que podemos considerar funcional, tiene un trasfondo histórico que demuestra un uso abusivo de los Estados más poderosos, y un irrespeto sobre los tratados y acuerdos internacionales cuando estos fueran de conveniencia a los elementos en el poder, que injerían forzosamente en Estados de su interés, con el fin de ignorar o alterar el ordenamiento jurídico en su favor, causando en el proceso desconcierto social y propiciando inclusive hasta masacres, véase el caso del Banana United Fruit Company y la masacre de las Bananeras en Colombia . Como consecuencia de este trasfondo de desconfianza, y plena consciencia de los abusos del pasado por parte de los Estados con más poder, el principio de no intervención se volvió un estándar del derecho internacional, cuya excepción esta únicamente supeditada a la responsabilidad de proteger.

Al ser el principio de no intervención una medida que protege la soberanía e integridad territorial de los Estados es un límite jurídico absoluto ante la jurisdicción de otros estados frente al estado titular. Para explicarlo en términos más simples, el principio de no intervención define que no se podrá injerir jamás un Estado, en los asuntos de otro Estado, y por lo tanto es incapaz de

ejercer su jurisdicción en esta, aun cuando esta se refiera respecto de la justicia, volviendo la persecución judicial en materia internacional, una dinámica de consentimientos y acuerdos, que no responde respecto de ninguna coerción, ni la posibilidad del uso de la fuerza, siendo las pretensiones que se buscara por estos medios, sustituidos por el papel que desarrollaban los llamados tribunales internacionales.

Al entrar a la doctrina, se vuelve de manejo común de una buena parte de los doctrinarios la idea de que para entender el principio de no intervención, primero debemos atender sobre que se puede considerar como tal, que se contempla como intervención, que resulta no estar consolidada en su definición por parte de la propia doctrina, con posiciones discrepantes respecto del concepto de intervención absoluta, que en pocas palabras, entiende que cualquier interacción de un Estado en los asuntos de otros se considera injerencia, y por tanto intervención, incluyendo hasta incluso las mediaciones, y otras posiciones más abiertas que entienden la intervención según los grados de injerencia.

Benítez (2015), docente de la escuela de Derecho de la Pontifica Universidad Católica de Valparaíso, habla en un artículo dedicado al principio de no intervención, acerca de lo que se puede englobar en la voz mediación, refiriéndose mayoritariamente sobre interacciones que implican el uso de medios políticos, económicos, jurídicos y militares, ya sea por coerción o no, con el fin de intervenir o injerir en asuntos, sean internos o externos, de otro Estado.

La posición expuesta por Benítez refleja que la intervención se puede entender como un intento de injerir, por cualquier medio que este sea pudiendo involucrar medidas meramente diplomáticas o comentarios, en los asuntos de otro Estado. Por lo tanto, el ejercicio no autorizado de la jurisdicción, una potestad estatal derivada de la autoridad y la soberanía, en otro Estado, es completamente inviable. La relevancia de esta dinámica para el caso reside en que la oposición que hace el principio de no intervención a la jurisdicción, limita por completo la capacidad de acción de ciertos Estados frente aspectos de la tecnología informática que tiene un desarrollo en dos jurisdicciones, ya que se requeriría en buena parte para que esta fuese efectiva, que las legislaciones de ambos Estados tengan líneas de acción similares, caso contrario, el accionar de la norma escrita se vuelve en extremo dificultoso para poder hacerlo efectivo, haciendo claro que del principio de no intervención se origina el conflicto de jurisdicciones, una problemática que aun a día de hoy no tiene una forma efectiva sobre su determinación salvo que exista una acuerdo específica sobre el procedimiento entre los países relacionados.

4.2.5 Interpol

La Organización Internacional de Policía Criminal (s. f) se define a sí misma en su portal web, en los siguientes términos:

> Somos una organización intergubernamental que cuenta con 194 países miembros. Ayudamos a la policía de estos países a colaborar entre sí para hacer del mundo un lugar más seguro.
>
> Para ello, les facilitamos el intercambio y acceso a información sobre delitos y delincuentes. También les ofrecemos apoyo técnico y operativo de diversa índole (¿Qué es la INTERPOL?, párrafo 1).

Existiendo desde 1923, la INTERPOL es un organismo internacional de asistencia recíproca entre organismos policiales. Esté no cuenta por sí mismo con un cuerpo oficial de actores policiales, ni actúan bajo una jurisdicción especifica cuando, por ejemplo, emiten una notificación roja, la cual por su nombre popular "boleta roja" da la impresión errónea de ser una orden de detención con legitimidad derivada de la propia autoridad intrínseca del organismo. El termino notificación es más adecuado, porque mientras que una boleta es un mecanismo que actúa por autoridad derivada de un organismo de justicia, la notificación es una solicitud a los organismos que conforman interpol en virtud de un orden judicial de un país solicitante, siendo la palabra solicitar el verbo rector de todo el actuar de la INTERPOL como organismo intergubernamental, pues sus actos son resultado de la colaboración, no del mandato y obligación. Citando la definición que el organismo tiene sobre la notificación roja "Una notificación roja es un aviso internacional sobre una persona buscada, pero no es una orden de detención". (INTERPOL, s. f, "Las notificaciones rojas", párrafo 4).

Esta aclaración es importante, porque corrige una de las posiciones más erróneas que existe en el imaginario popular acerca de la institución, que es el hecho de que la INTERPOL no actúa en ningún momento como un ente de detención particular ajeno a las fuerzas de seguridad de los países miembros. Su rol se rige exclusivamente el coordinar el funcionamiento de cada uno de estos organismos de manera conjunta. Esta condición lo invalida automáticamente para actuar como solución definitiva o supletoria al problema de supranacionalidad de los delitos informáticos que se trata en este trabajo, no al menos desde la intención de argumentar que esta institución suple la falta de convenios y tratados de colaboración internacional para la persecución de delitos

informáticos, pues como dice la organización en su portal web “INTERPOL no puede obligar a las autoridades encargadas de la aplicación de la ley de ningún país a detener a una persona objeto de una notificación roja. Cada país miembro decide qué valor jurídico otorga a una notificación roja, y cuál de sus organismos encargados de hacer cumplir la ley puede llevar a cabo las detenciones.” (INTERPOL, s. f, “Las notificaciones rojas”, ¿Estas personas son buscadas por la INTERPOL?, párrafo 2-3). Esto supone nuevamente, que el proceso penal pendiente, no tiene mayor garantía de colaboración con el país solicitante, más allá de voluntariedad del homónimo, que suele ser el escenario más común, pero no es una garantía fehaciente, no al mismo nivel de un convenio, el cual, si cuenta con fuerza vinculante entre las naciones, y sanciones contempladas en el derecho internacional en caso de su incumplimiento.

No obstante, si bien la INTERPOL no soluciona en su totalidad la problemática de la transnacionalidad. Tiene un valor enorme derivado de su rol como mecanismo de colaboración y apoyo que sigue brindando eficiencia a los procesos internacionales a través de la colaboración y apoyo que este ofrece. La colaboración ofrecida por el organismo es principalmente en términos de intercambio de información, extradiciones y temas procesales. El rol más usual que suele prestar este organismo, y el más fundamental, es hacer de un centro de apoyo en materia forense, de datos, búsqueda y notificación, sirviendo como base datos sobre individuos buscados por una jurisdicción exterior a través de su sistema de comunicaciones: I-24/7.

Sobre la base del último punto señalado, el rol de apoyo forense es donde yace uno de los más grandes aportes de la INTERPOL dentro del ámbito del derecho penal informático. Al ser un ente que opera globalmente, esta organización actúa en contacto continuo con delitos de carácter informática, experiencia de la cual se han servido como organización, lo cual las posiciona como uno organismo policial con mejor entendimiento sobre el fenómeno cibercriminal, expidiendo así normativas que buscan establecer protocolos de manejo respecto de estas problemáticas. Este entendimiento ha establecido como posición institucional el esfuerzo en “la creación de alianzas multisectoriales, como a posibilitar la cooperación de las fuerzas del orden a escala internacional.” (INTERPOL, s.f, “Ciberdelincuencia”, párrafo 4)

Como consecuencia que distinguimos puede tener la INTERPOL derivada de su posición, vale explorar los mecanismos los cuales se ha servido o ha producido para enfrentar la ciberdelincuencia; para poder reconocer y apreciar el valor de su experiencia, reflejada en sus obras y campañas; y apreciar como consecuencia si estas pueden ser adoptados por los organismos de

seguridad del Estado ecuatoriano para mejorar en materia relativa a su política pública.

4.2.5.1 Una breve historia de la relación INTERPOL-República del Ecuador

Ecuador se adhirió a la INTERPOL en 1962. El organismo es internacional, por lo cual, mantienen una presencia física en cada país que es parte del tratado. En Ecuador, esta unidad se encuentra en quito, integrada dentro del departamento de Investigaciones Criminales del Ecuador.

Actualmente, solo existe una notificación roja del Ecuador en la INTERPOL, la correspondiente a German Cáceres, recientemente capturado en la República de Colombia, expulsado, y entregado a las autoridades ecuatorianos, donde hoy permanece bajo su custodia.

4.2.5.2 Políticas de Concientización de la INTERPOL sobre la ciberdelincuencia.

- **#ElPróximoPuedeSerUsted**

El propósito de esta campaña de concientización centra sus esfuerzos en poner a la vista pública los peligros latentes derivados de las amenazas de extorción en línea. Las modalidades más comunes en estas actividades son la extorción sexual, el uso de Ramsomware y los DDoS (la sobrecarga de tráfico en un canal o servidor), los cuales explica en términos sencillos.

A través de un énfasis pesado en el constante acecho de los hackers hacia los usuarios, en búsqueda de una mínima apertura, un golpe de suerte o una vulneración cualquiera para poder atacar; es así como esta campaña logra sembrar el mensaje deseado en los internautas. Ser precavido, usar el sentido común y no ingresar a lugares sospechosos son comportamientos resultantes.

La campaña también ofrece acciones preventivas y de acción que los usuarios pueden tomar, con efectividad probada, para evitar ser víctima de estos ataques, algunos ejemplos: copias de seguridad, antivirus, descargar con distribuidores autorizados

- **#OnlineCrimeIsReal**

Conscientes sobre el valor que la población le da los delitos informáticos, un menosprecio sobre su importancia o siquiera su posibilidad de suceder. La mentalidad del ciudadano está atada a un plano estrictamente físico, completamente inconscientes que el delito puede alcanzarles aun desde la remotidad de otro continente a través de un medio completamente inaccesible en termino físicos, la informática. Esta campaña toma esta problemática, y acerca la realidad vigente, una exposición sobre el cómo ya nada puede escapar de la tecnología, y por lo tanto un delito informático puede significar igual o mayor peligro que un crimen normal, esto a través de exponer sus modalidades, sus consecuencias, y el cómo estos mecanismos se aprovechan de esta

preconcepción errónea.

- **#SolouUnClic**

Solo un Clic es una campaña que entiende y expone como la ignorancia dentro de las redes puede llegar a ser sumamente dañina en las redes, el mínimo paso en falso, o en este caso, tanto solo un clic errado, sin conocimiento, puede abrir la puerta a delincuentes informáticos, una ventana de oportunidad que es subestimada por el público en general, que da por sentado la seguridad intrínseca de sus interacciones en línea y sobreestima su conocimiento sobre el ecosistema informático, exponiéndose así a potencial peligro. Al mismo tiempo, basta un clic para poder tomar las medidas adecuadas que garanticen tu seguridad, un clic en la responsabilidad del usuario. La campaña fue una de concientización sobre las amenazas varias y constantes que provienen desde las entrañas de la web; y la forma en que podemos protegernos ante ellas.

4.2.6 Política Criminal

La ley escrita es sumamente eficaz para dar una pauta sobre qué acciones tomar sobre un determinado caso, o que conductas suprimir. No obstante, la ley escrita sufre cuando existen desfases entre lo que dice la norma, y lo que se plasma en la realidad. Esto se hace especialmente relevante en el ámbito penal, donde los términos escritos en la norma son mucho más estrictos en su interpretación, y por tanto no dan lugar a configurar como delito, nada que este más allá de lo que las leyes han descrito. Sin embargo, como herramienta para poder reducir el impacto de esta problemática, tenemos la política criminal, que actúa como un mecanismo que busca disuadir y persuadir a los ciudadanos de no involucrarse en dichas acciones no tipificadas, sin alterar la ley penal, o el debido proceso.

La Política Criminal, es una aplicación de la potestad de política pública que posee el Estado central, por lo que es indispensable definir en qué términos se maneja esta. La Constitución de la República del Ecuador (2008) indica sobre que esta que:

> Art. 85.- La formulación, ejecución, evaluación y control de las políticas y servicios públicos que garanticen los derechos reconocidos por la Constitución, se regularán de acuerdo con las siguientes disposiciones:
>
> 1. Las políticas públicas y la prestación de bienes y servicios públicos se orientarán a hacer efectivos el buen vivir y todos los derechos, y se formularán a partir del principio de solidaridad.

> 2. Sin perjuicio de la prevalencia del interés general sobre el interés particular, cuando los efectos de la ejecución de las políticas públicas o prestación de bienes o servicios públicos vulneren o amenacen con vulnerar derechos constitucionales, la política o prestación deberá reformularse o se adoptarán medidas alternativas que concilien los derechos en conflicto.
>
> 3. El Estado garantizará la distribución equitativa y solidaria del presupuesto para la ejecución de las políticas públicas y la prestación de bienes y servicios públicos.
>
> En la formulación, ejecución, evaluación y control de las políticas y servicios públicos se garantizará la participación de las personas, comunidades, pueblos y nacionalidades.

Mas que entenderlo como una política que busca perseguir el crimen, pues esto se da por sentado ya que el Estado es el ejecutor de la ley penal, la política pública criminal es más respecto al tratamiento de la problemática criminal, antes de que esta se consume, involucrando temas como la preparación logística, la capacitación del personal de policía y el monitoreo de acciones sospechosas. En otras palabras, son las decisiones políticas que toma el Estado para poder luchar contra la delincuencia, sin enforzar ninguna figura o tipo penal vigente, a través de la mejora de la seguridad, o, de estarse aun en planeación, pararlas, configurándolas como tentativas en el proceso.

Borja Jiménez (2003) hace un acercamiento respecto de la política criminal como concepto, de como esta se define por el derecho penal, y de cómo este último es un muro que define el margen de acción de la primero, ofreciendo la siguiente perspectiva

> El Derecho penal era concebido como una ciencia estructurada en torno a unos principios de garantía de las libertades del ciudadano (legalidad, culpabilidad, intervenci6n mínima, etc.), sistematizada con una firmeza 1ogica inquebrantable y cuya finalidad estaba más próxima a limitar al poder punitivo que a tutelar a la sociedad. La Política Criminal, por el contrario, se contemplaba como un conjunto de estrategias destinadas por los poderes públicos a frenar altas tasas de criminalidad. (…) esos poderes públicos intentaran a través de una determinada política criminal auspiciar al máximo la seguridad ciudadana, y el Derecho penal pretenderla limitar esa actividad del Estado para respetar los derechos de los individuos sospechosos, acusados o condenados en relaci6n con la perpetraci6n de un delito. (p. 2)

Esta política criminal, es también un instrumento para mesurar respecto de las capacidades operativas de los responsable de dicho fenómeno, por lo tanto, es a su vez medida de contención,

y mecanismo de medición, un punto que provee ventajas a través de la información que estas nos arrojan, para que en coordinación con el resto de políticas públicas, se pueda atacar al fenómeno desde la conceptualización en la sociedad erradicando sus causas y purgando sus estructuras más fundamentales o de apoyo, como lo puede ser el narcotráfico con la prostitución, tratando de buscar siempre la piece de resistence en el esquema a la cual atacar a través de medios externos al fiscal y de seguridad, como lo son la educación y los programas de ayuda social.

4.2.7 Propiedad Intelectual

La propiedad intelectual se ha configurado como uno de los problemas que más agravian al internet desde los tiempos de su creación. Como se ha señalado con anterioridad, la libertad casi anarquista de la red temprana llevo a un ambiente en el que la distribución ilegal de contenido se volvió supremamente conveniente. La falta de jurisdicción, legislación y de estándares de seguridad claros, en la etapa de un temprano internet, llevaron a que los grupos de distribución de contenido sujeto a derechos de autor se convirtieran en auténticos gigantes tecnológicos y empresariales, véase el caso de Napster, Ares, o Megaupload.

La propiedad intelectual podemos entenderla desde el concepto que formula Canaval Palacios (2008), como aquella propiedad que se le extiende a las cosas inmateriales o incorpóreas, siempre hablándolo desde la perspectiva desde la perspectiva de la ideación y concepción de un producto incorpóreo. Cabe mencionar, que el derecho intelectual es un término que se aplica únicamente sobre los productos inmateriales, pues lo material se sujeta al derecho de patentes. Es decir, en la reproducción de un libro, la propiedad intelectual no interviene en el material, ni en el producto del libro como tal, sino por la reproducción fidedigna de un producto no material que es la idea del libro, la historia.

Al ser la informática un ecosistema, estrictamente sujeto a la inmaterialidad de su contenido, siendo la única parte material el ordenador, como arquitectura que lo sostiene; está ligado muy profundamente a la propiedad intelectual y al derecho que lo regula, y cuya importancia reside en su protección a la producción cultural y científica.

La Organización Mundial de la Propiedad Intelectual (s. f) explica al derecho de autor en los siguientes términos

> En la terminología jurídica, la expresión “derecho de autor” se utiliza para describir los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y

las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos.

Reflejando como el aspecto informático se ha acoplado a estas concepciones, ligando el derecho de propiedad intelectual con el derecho informático de forma inseparable para el futuro venidero.

Cuando a Derechos de propiedad intelectual se refiere en informática, las perspectivas sin duda variopintas entre sí. Como explica Rodríguez (2013) la doctrina tiene tres perspectivas, las cuales difieren la una de la otra, acerca de los derechos del software. La primera de estas sostiene que esta se acoge a la normativa de patentes de invención, la segunda formula que estos pertenecen dentro de los derechos de autor, y el tercero de estos indica que estos tienen una caracterización propia, probablemente derivando de las particularidades del software (p. 42).

El derecho de propiedad intelectual y el derecho informático han tenido un lazo muy profundo desde la década de los primeros años de la popularización de los dispositivos informáticos y el uso del internet como plataforma de distribución de información. Anterior a la existencia de estos, la adquisición de productos sujetos a derechos de autor se limitaba a la compra de productos oficiales emitidos por el titular de estos a través de un distribuidor intermediario, siendo la reproducción no autorizada de estos mucho más complicado debido a la falta de accesibilidad de las herramientas requeridas para poder realizar el duplicado de los productos sujetos a derechos de autor, fueran estos libros, música, productos audiovisuales de todo tipo o imágenes, y las dificultades que existía para distribuirlos debido a que al ser productos virtualmente de contrabando, solo podían intercambiarse o repartirse a un grupo limitado de gente que habitaban el mismo nicho. No obstante, la penetración tecnológica que sucedió durante la segunda mitad del siglo XX, haciendo especial énfasis en el internet como la piedra angular de este, cambio por completo el paradigma. Las nuevas tecnologías rompieron la formula ya que solucionaban el problema de acceso a las herramientas de captación y modificación, a través de la digitalización de los productos audiovisuales y la edición o modificación de estos mismos; y solventaban de manera espectacular el problema de la distribución, sirviendo el internet como un punto logístico digital de escala global que ofrecía a su vez, anonimato e impunidad consecuente. Como explicarían Altmark y Molina (2012) “Los valores libertarios de quienes crearon y desarrollaron Internet, a saber, los investigadores académicos informáticos, los hackers, las redes comunitarias contraculturales y los emprendedores de la nueva economía, determinaron una arquitectura abierta

y de difícil control" (p. 37) siendo estas características, caldos de cultivos más que fértiles para la proliferación de una temprana, creciente y vibrante industria digital basada en la piratería.

A exponer de Rodríguez (2013) la piratería de ejemplares es el caso más simple que se configura cuando sucede la reproducción de su una obra sin autorización del titular de su autoría teniendo por modalidades la falsificación, la copia de software usurpado con propósito comercial, la copia de usuarios corporativos evadiendo el costo de la licencia y la copia realizada de usuarios finales para uso propio. A esto cabe sumarle las figuras del plagio no elaborado, que es la copia que se realiza sin duplicar en si el ejemplar original, resumiéndose únicamente a alterar el titulo o elementos menores del producto con el fin de presentarlo como uno totalmente diferente; el plagio elaborado, que es un grado superior al anterior en el intento de modificar la obra de forma que el producto original pase desapercibido y pueda ser distribuido sobre una identidad diferente y confundir al consumidor final; finalmente el "look and feel" hace referencia a que el producto secundario evoca una imagen y sensación de trabajo similar al producto secundario (p. 44-45).

4.2.8 Delito y delito informático

Para el presente trabajo es esencial establecer una definición de lo que delito se refiere.

El Diccionario Jurídico Enciclopédico (2005) ofrece sobre el delito dos grupos de definiciones. El primero "definiciones prejurídicas o condiciones de las legislaciones" (p. 433) y el Segundo "definiciones dogmáticas, referidas a una legislación positiva" (p. 433). En la primera contempla fundamentación filosófico-jurídica; la segunda, un enfoque sociológico naturalista.

Para Muñoz (2004, p. 205, como citado en Machicado, 2010, p. 2) el delito es más una valoración de la conducta sometida a condiciones éticas propias de la clase dominante. Machicado (2010, p. 3) explica que existen concepciones formales y substanciales del delito. La primera, la formal, establece al delito como una conducta humana en contra de ley que mando o prohíbe. Por otro lado, la substancial contempla que existen elementos presupuestos que determinan si una conducta humana puede considerarse delictiva. Esta debe de ser antijurídica, culpable, y sancionada con una pena criminal.

El delito es considerado como un fenómeno y como ente jurídico. Ambas concepciones ofrecen una perspectiva bastante concreta sobre el delito. El primero trabaja sobre la línea perspectiva que contempla al delito como un parte inevitable de la naturaleza social y por tanto estima que su existencia está ligada a razones propias de la naturaleza social del acto y como esta causa conflictos o desperfectos en el sistema social con el que interactúa. En resumidas palabras,

el delito es un hecho social y se considera como tal según el grado de amenaza social que este implique.

En contraste, la idea de que el delito es un ente jurídico establece que, para la consideración del mismo, la actitud a estimar debe cumplir con el requisito mínimo de ser una conducta que afecte, viole u omita un derecho establecido, operando la figura de delito sin considerar necesariamente sobre la concepción moral o ética que tiene la sociedad al respecto, estimando como punto más importante la valoración de una afectación real de los derechos legalmente constituidos. Probablemente, teniendo presente que la realidad moral o ética de una sociedad no es un valor absoluto o inmutable, y que por tanto someter la valoración de un hecho a una idea tan heterogénea o ambigua no es una buena base legal.

Para la legislación ecuatoriana, el Código Orgánico Integral Penal (2014) los delitos son un parte del conjunto de infracciones penales, la legislación penal la define en su Art. 19 dictando "Delito es la infracción penal sancionada con pena privativa de libertad mayor a treinta días" (p. 38) y caracterizándose también por jerarquía según las características que el mismo Código Orgánico Integral Penal le entrega a la Infracción penal, donde el delito se incluye, en su Art. 18 que dicta que estas serán conductas típicas, antijuridica y culpable con sanción prevista en el Código Orgánico Integral Penal.

El mundo ha cambiado drásticamente en las últimas décadas. La tecnología ha transformado nuestro contexto de una manera tan determinante que vuelve imposible el mantener las legislaciones al día con los cambios. En cuestión de un lustro, hasta la más innovadora de las normas podía quedar completamente obsoleta.

Esto no es un problema en sí mismo de planteamiento de las normas, simplemente se vuelve imposible redactar una norma escrita que pueda contemplar la infinidad de probables cambios o nuevas tecnologías que la innovación puede escupir a la realidad jurídica.

La opción más viable se vuelve entonces se encuentra no enfocarse en sí mismo en los modos de delincuencia informática, y centrarse mucho más en las consecuencias comunes que estas pueden tener o los derechos que independientemente del medio se violan, teniendo como diferenciador como elemento constitutivo su realización a través de medios informáticos o electrónicos.

Con entendimiento de que los delitos informáticos tienen una intromisión internacional, y contemplando que, como consecuencia de lo mencionado, las soluciones jurídicas meramente

locales no funcionan adecuada, se abre una necesidad de establecer mecanismos de cooperación jurídicos de carácter internacional. Acuario del Pino (2001) señala como las naciones unidas consideraban que el problema se eleva a una escena internacional y que se configuran en crímenes transnacionales, señalando en las complicaciones de la cooperación para perseguirlos, la falta de una nomenclatura uniforme, tanto en las conductas como en las definiciones, falta de capacitación de los actores de justicia, la ausencia de tratados de cooperación y extradición. (p. 30). Este escenario era una realidad cuando las Naciones Unidas se pronunciaron en el Manual de Prevención y Control de Delitos Informáticos, y persiste a tiempos actuales, con especial énfasis en los Estados pertenecientes al tercer mundo. Si bien se sumaron reformas y leyes que permitían juzgar los delitos. La falta de un marco de cooperación internacional volvió mucho más dificultosa la persecución de los delitos. A estos cabe agregarle, la poca capacitación que se ha reservado para las fuerzas del orden en el tema, que termina traduciéndose a una evidente incapacidad operativa.

Las categorizaciones de los delitos informáticos, se estructurarán siguiendo las formas acogidas en el convenio sobre ciberdelincuencia de Budapest, por ser este un marco transnacional jurídico que ha surtido efectos considerables en la Unión Europea y por qué ha sido además un marco jurídico que ha servido como base de múltiples legislaciones ajenas a la misma Unión Europea, como las vecinas Colombia y Perú, que se adhirieron a los términos de la misma en orden con los tratados de libre comercio que estos subscribieron con la UE. Esto a tomar en cuenta que uno de los objetivos de este trabajo es mostrar las zonas más porosas de la legislación ecuatoriana y de su procedimiento, a través de someterla a un contraste duro frente a otras legislaciones, prestando además este convenio un marco de cooperación internacional que puede ofrecer valor de análisis para la legislación nacional.

Cabe señalar, además, que Ecuador no se encuentra adherido a este tratado, aunque es observador del mismo, por lo cual se analizara de igual modo en las conclusiones los beneficios que podría suponer la adhesión de la república al mismo.

4.2.9 Mecanismos de aplicación de la ley penal

La exploración de los efectos de una legislación tiene una obligación directa de revisión crítica respecto de los medios o mecanismos de aplicación de los cuales la mencionada de depender para superar el umbral de la mera literalidad de su existencia, hacia un efecto en la realidad.

Entendiendo que el presente trabajo abarca exclusivamente un arco penal, se vuelve entonces menester identificar y comprender los elementos que están ligados a este ámbito dentro

del ordenamiento jurídico ecuatoriano.

El estado, personificado en institución republicana en el Ecuador, es el ostentador del monopolio absoluto del uso de la fuerza. Esta es una de las premisas fundamentales de la teoría estatal moderna, esta potestad exclusiva tiene dos vertientes de legitimidad y uso en la realidad jurídica. La primera, salvaguardar la integridad del estado constitucional, es decir una cuestión primordial de supervivencia; y la segunda, la coerción como mecanismo de garantía del efecto de las leyes y el consecuente cumplimiento de la amenaza de fuerza consecuencia del incumplimiento.

La Función Judicial es uno de los cinco poderes estatales, institucionalizada en la idea de que la justicia emana del pueblo, no del estado, y que este únicamente la ejerce como facultad. Esta breve concepción es la idea más fundamental sobre la que se estructura la justicia dentro de las fronteras de la república.

No obstante, la potestad punitiva no es discrecional, pues está sujeta estrictamente por las condiciones que el marco constitucional ha dictado para el efecto, y en los mismos términos, no está en el estado como concepto absoluto el ejercer todas las posiciones del proceso que llevan a la consecuencia del ejercicio de la fuerza, encontrándose el ejercicio de este poder dividido en roles distribuidos a organismos diferentes de la estructura estatal.

La Función Judicial es uno de los cinco poderes estatales, institucionalizada en la idea de que la justicia emana del pueblo, no del estado, y que este únicamente la ejerce como facultad. Esta breve concepción es la idea más fundamental sobre la que se estructura la justicia dentro de las fronteras de la república.

La deliberación sobre los hechos a someter a supresión estatal, encarnado en la institución de la Función Judicial regulado en su estructura formal por el Consejo de la Judicatura. El ejercicio de la acusación en los delitos de acción pública, apreciando el estado que las afectaciones derivadas de los actos penalmente punibles son de afectación social, asignado en funciones y ejercicio a la Fiscalía General del Estado. Por último, la institución que conceptualiza la potestad del uso civil e interno del monopolio de la fuerza, estructurado en la figura de la Policía Nacional.

4.2.10 Fiscalía General del Estado

Existen ciertas ofensas que por las implicaciones de sus consecuencias que estas tienen en el tejido social exceden la afectación de la víctima como particular, y se constituyen como una ofensa contra la sociedad misma. Estos son denominados delitos de acción pública.

Dentro de legislación penal ecuatoriana la fiscalía general del Estado se constituye como el

organismo autónomo a cargo del ejercicio de la acción acusatoria en representación del interés general. Una situación sustancialmente significativa puesto que la Fiscalía es un ente que no actúa como el estado, ya que puede actuar en contra de él.

La Constitución de la República del Ecuador configura el mencionado ente en su Artículo 195

> La Fiscalía dirigirá, de oficio o a petición de parte, la investigación preprocesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal. (Constitución de la República del Ecuador, 2008, Artículo 195, p. 201)

Al ser la Fiscalía el solo mecanismo impulsor de delitos de acción pública es al primer órgano al que debemos observar para el ejercicio de la ley penal. Al estar la formulación de cargos a la orden de este organismo, se está poniendo en manos de la fiscalía el impulso inicial, y el más importante, sobre los delitos.

Entendiendo que los mecanismos procesales son aquellos que vuelven efectiva a una ley, se entenderá que el des atendimiento, desactualización e ineficiencias procesales en la fiscalía afectará inevitablemente a la persecución de los delitos.

Teniendo presente que la realidad informática es un nuevo universo para el derecho penal ecuatoriano, y que las reformas percibidas en la ley tienen fecha reciente, pueden existir problemas derivados de la falta de capacitación que desencadenen a su vez complicaciones procesales o probatorios relacionados a estos delitos, siendo así un obstáculo en su papel preventivo o disuasivo de los tipos penales. Este punto es relevante, ya que tiene una directa vinculación en el estudio de casos que se detallaran más adelante, más específicamente el primero de estos, pudiendo evidenciarse cuestiones derivadas del desconocimiento de las formas propias de la informática de manera rotunda en la forma en que llevo la Fiscalía este caso, que cabe mencionar tenía relevancia mediática como un factor presión externo.

4.2.11 Policía Nacional

La Policía Nacional es uno de los dos brazos armados que posee el estado, y en las concepciones doctrinarias del monopolio del uso de la fuerza, son uno de los mecanismos de aplicación y ejercicio de susodicho monopolio estatal.

La Constitución de la República del Ecuador las define en los siguientes términos

> La Policía Nacional es una institución estatal de carácter civil, armada, técnica, jerarquizada, disciplinada, profesional y altamente especializada, cuya misión es atender la seguridad ciudadana y el orden público, y proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional. (Constitución de la República del Ecuador, 2008, Art. 163)

Como garantes de la seguridad ciudadana, las fuerzas armadas están activamente involucradas en la prevención, persecución y sanción de los delitos. Estando ligados en un rol colaborativo con la función judicial.

El propio Código Orgánico de la Función Judicial (2009) la encadena sumisamente en su artículo 30, inciso segundo que dicta así "La Policía Nacional tiene como deber inmediato, auxiliar y ayudar a los jueces, y ejecutar pronto y eficazmente sus decisiones o resoluciones cuando así se lo requiera" (Código Orgánico de la Función Judicial, 2009, art. 30).

¿Por qué esto es relevante? La respuesta es simple. La policía nacional, según lo ha desarrollado la ley, es un órgano que colaborativo de la justicia, siendo una extensión del poder judicial a través de la colaboración.

Existe una especial relación que esta tiene con la Fiscalía General del Estado, misma que manda la Constitución (2008) de la siguiente manera "Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial;" en su artículo 195, segundo inciso. (Constitución de la República del Ecuador, 2008, Artículo 195).

Esta relación tiene como consecuencia que la Policía nacional se maneje a la vez como una extensión operativa de los agentes fiscales, y un organismo de investigación de apoyo, encarnado en la Policía Judicial y demás personal investigativo. Rol que lo vincula directamente con la obtención, análisis, resguardo y entrega de evidencia y medios probatorios; volviéndolo así otro punto a observar respecto de las capacidades que tiene el personal policial para poder manejar adecuadamente estas, cuando de material digital hablamos. Además de que la vinculación entre estos dos órganos enlaza de algún modo las afectaciones de la Fiscalía, a las de la Policía hasta cierto grado, donde la falta de conocimiento y capacitación por parte de los fiscales puede llevar a discrepancias o desestimaciones entre policía y fiscalía, o la falta de capacitación del personal policial puede estropear los avances e investigaciones llevadas por fiscalía.

4.3 Análisis en base al convenio

4.3.1 Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Consciente de que la influencia de los medios informáticos ha alcanzado incluso los medios a través de los cuales manejamos nuestra vida íntima, en especial a través de las redes sociales y correos electrónicos que han suplantado otros mecanismos sociales de comunicación. En consecuencia, la norma ha reconocido la importancia de estas plataformas y su influencia sobre nuestra intimidad y confidencialidad

El convenio de cibercriminalidad de distingue este mismo en los siguientes tipos:

Art. 2 Acceso ilícito

A exponer del Convenio de Cibercriminalidad de Budapest este se expone como:

> Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegitimo a todo o parte de un sistema informático. Las Parte podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático. (Convenio sobre Cibercriminalidad, 2001, art. 2, p. 4)

El propósito de este enunciado es exponer una clara salvaguarda sobre la capacidad de acceder a la información que dentro de un sistema informático se encuentra codificada. La salvaguarda sobre este acceso está en concordancia intima con el derecho a la confidencialidad y a la intimidad al ser la información manejada en los dispositivos electrónicos de carácter personal, delicada y estratégica para el usuario titular u ocupante del equipo.

Entendemos el acceso ilícito como la capacidad de acceder a un dispositivo, base de datos, servidor o cualquier tipo de arquitectura electrónica que permita en ella almacenar datos informáticos, a través de medios que vayan en desconocimiento de los titulares o autorizados para el ingreso a este en contrario de su voluntad. Una irrupción no autorizada o forzada del espacio virtual. El convenio contempla adecuadamente que existen niveles de irrupción de estos espacios, así que deja a libertad de los Estados el establecer los requerimientos respecto del propósito o nivel de seguridad a violar que se ha de considerar al momento de tipificar el delito en sus respectivas legislaciones.

La legislación ecuatoriana contempla una figura similar a través del Art. 234 de su Código Orgánico Integral Penal

> Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. (Código Orgánico Integral Penal, 2014, art. 34, p. 78-79)

En este artículo se observan elementos comunes entre la legislación ecuatoriana y la convención, como la ilegitimidad del acceso, la obtención o explotación de datos informáticos y la intención de con estos o través de este acceso llevar a cabo otras actividades delictivas, aunque en la norma ecuatoriana se es mucho más específico sobre cuales actividades ilegitimas se estimaran como constitutivas de este. Cuando la convención se refiere a intenciones delictivas, y por tanto como objetivo último de estas mismas a actividades delictivas, permite una ventana de ambigüedad que da espacio a que se acople en ella cualquier actividad que dentro de la legislación interna considere delito, dando así facilidades para que las legislaciones de los Estados que a ella decidan acoplarse, tengan un margen de acoplamiento más flexible, al permitir que cualquier delito que este tipificado, que se realice o tenga parte de sus medios de realización dentro del ambiente informático, pueda englobarse dentro de esta.

Art. 3. Interceptación ilícita

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que trasporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con contención intención delictiva o en relación con un sistema informático. (Convenio sobre Cibercriminalidad, 2001, p. 4-5)

El uso continuo y sistemático de líneas ´de comunicación informáticas o a través de medios electromagnéticos, ha vuelto a su vez la legislación sobre estas mismas conexiones un punto de preocupación, en especial cuando de información personal, sensible o estratégica se trata. Como consecuencia se formula que la intercepción ilícita de la información que por estos medios se traslada ha de tipificarse en termino comunes. Entendemos la intercepción ilícita del mismo modo que con el acceso ilícito como la concesión de los mencionados datos a través de la irrupción, vulneración o ingreso no autorizado a estos canales para la sustracción de información, siendo este contrario a voluntad de quien tenga derecho de autorización o en su desconocimiento. La legislación común en los términos del convenio contempla que se puede contemplar como delito tanto solo la acción de irrumpir a estos canales, como se puede a su vez establecer como elemento constitutivo la intención de hacer uso o explotación de este acceso ilegitimo para provecho delictivo.

Art. 4.- Ataques a la integridad de los datos

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resultan necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo comporten daños graves. (Convenio sobre Cibercriminalidad, 2001, p. 5)

Entendida la importancia de los documentos, código o tokens que a través de medios informáticos se muevan, es menester que le legislación contemple que la alteración no autorizada, ilegitima y viciada de estos mismos. Tomando en cuenta que, a los ojos de las legislaciones, los documentos digitales pueden llevar un mismo nivel de responsabilidad como los documentos físicos, y entendiendo que la alteración del contenidos de estos puede conllevar perjuicios tanto a las personas que los emiten, como a las personas que los receptan, mencionando además que datos informáticos como el código fuente pueden ser la columna vertebral de enteras arquitecturas informáticas y cuyo mal funcionar pueden generar perjuicios económicos y legales importantes. El convenio de ciberdelincuencia estima que debe existir uniformidad respecto de la tipificación de esta actividad delictiva, reservándose únicamente las partes la posibilidad de determinar respecto de la gravedad de estos, pero no respecto de la forma e intención del mismo.

Art. 5.- Ataques a la integridad del Sistema

> Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos. (Convenio sobre Cibercriminalidad, 2001, p. 5)

Por múltiples razones entre las que se pueden citar ataques con intención deshabilitar las capacidades operativas de una nación, hasta el imposibilitar el correcto funcionamiento de una plataforma de registro electoral, los ataques a la integridad de los sistemas informáticos se han vuelto una amenaza muy real a contemplar tanto como una cuestión de seguridad nacional, en el peor de los escenarios, hasta una amenaza a la seguridad personal, en los casos más particulares. Por tanto el integrar este tipo penal, permite una herramienta de rápida identificación respecto de los modos con los cuales son inhabilitadas o afectadas estos sistemas, mientras que da una base legal para para poder hacer una persecución más efectiva cuando estos mismos ataque provienen del exterior de la República, cosa común debido al bajo nivel de seguridad informática y educación informática de la región, y a la naturaleza transnacional de estos ataques que comúnmente suelen venir desde el extranjero.

Art. 6.- Abuso de Dispositivos

> (…) 1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima de los siguientes actos:
>
> a. La producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
>
> i. Cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presento Convenio.
>
> ii. Una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,
>
> Con intención de que sean utilizadas para cometer cualquiera de los delitos contemplados de los artículos 2 a 5; y

b. La posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente articulo con la intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente articulo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo. (Convenio sobre Cibercriminalidad, 2001, art. 6, p. 5-6)

Considerando la importancia estratégica que ha adquirido tanto software, es decir aquellos programas que trabajan internamente dentro del ordenador; como hardware, elementos y arquitecturas tecnológicas físicas que sirven para interactuar y sostener los primeros; se ha vuelto de necesidad esencial establecer la prohibición no solo ante la comisión de los delitos, sino ante el desarrollo mismo de los elementos que puedan actuar como medios tecnológicos para poder realizar la actividad delictiva o abusar de las vulnerabilidades del sistema. Dentro de estos elementos encontramos desde el malware, pasando por la información filtrada o interceptada, contraseñas de acceso transmitidas ilegítimamente. Sin embargo, probablemente pensando en la ambigüedad de que abarca el desarrollo de programas o herramientas para el abuso, y que la distribución de información filtrada suele ser de suma importancia para procesos investigativos, la convención establece que los términos antes mencionados, solo sujetaran a responsabilidad penal si es que estos fueren medios para el cometimiento de los delitos descritos en los artículos 1 al 5 de la misma.

4.3.2 Delitos informáticos

Definido claramente el delito, el siguiente paso para este trabajo será el definir como se contempla el delito informático.

Consciente de la cambiante naturaleza de la tecnología, las TICs y la informática, Hernández Díaz (2009, p. 231) explica las definiciones a lo largo del tiempo que se dieron respecto del derecho informático exponiendo como las primeras definiciones de delito informático se relacionaban cualquier incidente asociado a ordenadores en el que la víctima sufrió un daño, y el autor pudo u obtuvo beneficio. También expone como para Romeo Casabona, el termino delito le parecía inadecuado pues es una definición especifica que no se ajusta a la totalidad de conductas que se suelen clasificar como delitos informáticos, argumentando que sus modos de comisión suelen ser bastante heterogéneos salvo por el hecho de involucrarse en medios informáticos, argumentando que la delincuencia informática, es un término más flexible que permite incluir tanto a las conductas tipificadas como las que a pesar de no estarlo, merecen serlo de lege ferenda (p. 234).

Téllez (2009) también se acoge a la dificultad de definir el delito informático debido a lo cambiante de la tecnología, y ofrece como definición "En ese orden de ideas, según el caso, los delitos informáticos son actitudes ilícitas que tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin (concepto típico)" (p.188).

También ofrece como características su tendencia a ser conductas criminales de cuello blanco, ser ocupacionales, ser acciones de oportunidad, provocar serias perdidas informáticas, ofrecen facilidades de tiempo y espacio para su cometimiento, son muchos casos y pocas denuncias, de difícil comprobación, son dolosos o intencionales en su mayoría, ofrecen facilidades a los menores, y crecen en su proliferación.

Parker (1996 como se cita en Acurio del Pino, 2001) define "todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio"

El Convenio de Ciberdelincuencia de Budapest, contempla el delito informático en los siguientes términos.

Art. 7.- Falsificación informática

> Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos con independencia de que los datos sean elegibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal. (Convenio sobre Cibercriminalidad, 2001, art. 7, p. 6)

Apreciando adecuadamente que, a ojos de la legislación, y por haberse involucrado el mundo informático en conflictos legales, los mensajes o datos informáticos pueden tener un peso legal que les habilita a actuar como pruebas frente a procesos judiciales y a reclamos respecto de obligaciones legales. El convenio ha considerado importante darle un tipo especifico al acto de realizar modificaciones, sean estas ediciones, supresiones o agregados respecto de los mensajes informáticos, con el fin de alterar su sustancia, pues se entiende que la pretensión es presentar un texto contrario a la realidad y que por tanto contenga una actitud de dolo a través del engaño que genera como consecuencia un perjuicio para quien lo aqueja, respondiendo así de manera adecuada este tipo a la problemática que supone la alteración de mensajes ya sea en reclamos legales, o en exposición pública para denuncia social, pudiendo tener graves implicaciones sobre la imagen del individuo.

Art. 8.- Fraude informático

> Las Partes adoptaran las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:
>
> a. La introducción, alteración, borrado o supresión de datos informáticos;
>
> b. Cualquier interferencia en el funcionamiento de un sistema informático,
>
> Con la intención dolosa o delictiva, de obtener de forma ilegitima un beneficio económico para uno mismo o para otra persona. (Convenio sobre Cibercriminalidad, 2001, art. 8, p. 5)

La introducción de la informática, sus dispositivas en la vida social y su uso activo dentro las múltiples áreas de la misma abrieron un mundo de posibilidades para poder cambiar los paradigmas sobre las actividades que hasta ese punto se realizaban de manera persona a persona.

Ahora, estas acciones podían ser fácilmente realizadas a través de una interfaz neutra con la cual se podía ahorrar tiempo y por tanto productividad. Cabe mencionar que buena parte de este acercamiento hacia la integración tecnológica tenía una fuerte base en la superación de la desconfianza inicial sobre la cual se manejaba internet, volviéndose de este modo más accesible.

Aun así, la integración de antiguos tramites, procedimientos y actividades licitas dentro de la esfera informática, termino de igual modo por trasladar las actividades ilícitas a la misma, que se aprovechaban especialmente de las vulnerabilidades que se derivaban de la falta de conocimiento del público general sobre la seguridad y complejidad de la red, las vulneraciones en sistemas informáticos arcaicos, la facilidad del anonimato, y la transnacionalidad que había de por medio, permitiendo el florecer de actividades como la estafa o el fraude, que se aprovecharon de manera destacada del ambiente de comercio y otras actividades que, previa existencia de legislación, basaban su comportamiento mayormente en la confianza.

Como consecuencia, los usuarios fueron víctimas de múltiples estafas y fraudes informáticos. Conocido es el caso de estafa del príncipe nigeriano, o timo 419-que se refiere al artículo del código penal nigeriano que lo tipifica- que implicaba una modalidad de estafa.

En vista de los perjuicios que estas actividades generan sobre los usuarios el Convenio -que cabe mencionar se formuló en 2004, año en el cual estas actividades se encontraban aun en auge- estimo que existía gran importancia en formular un tipo, que enfrascara dentro de él la conducta delictiva del fraude, probablemente pretendiendo que a través de la formulación del mismo dentro del marco, también se ofrezca una base solidad para poder sobrepasar el problema de la transnacionalidad de estos delitos, al volver el tipo penal en una parte de la legislación interna de cada uno de los miembros.

4.3.3 Delitos relacionados con el contenido

Art. 9.- Delitos Relacionados con la Pornografía Infantil

1. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos

    a. La producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. La oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

c. La difusión o la transmisión de pornografía infantil a través de un sistema informático;

d. La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;

e. La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A Los efectos del párrafo 1 anterior, se entenderá por pornografía infantil todo material pornográfico que contenga la representación visual de:

a. Un menor adoptando un comportamiento sexualmente explicito;

b. Una persona que parezca un menor adoptando un comportamiento sexualmente explicito;

c. Imágenes realistas que represen a un menor adoptando un comportamiento sexualmente explicito.

3. A los efectos del párrafo 2 anterior, se entenderá por menor a toda persona menos de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las partes podrán reservarse el derecho a no aplicar, en todo o en parte los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2. (Convenio sobre Cibercriminalidad, 2001, art. 9, p. 6-7)

Uno de los delitos que de mejor manera se ha tratado dentro de las legislaciones latinoamericanas, puesto que esta está enmarcada dentro de una problemática que tiene una está persecución mucho más exhaustiva por parte de los Estados debido al nivel de rechazo que esta tiene a un nivel moral por parte de estas sociedades, que es en este caso, los delitos sexuales, con especial énfasis en los que exponen contenido sexual relacionado a menores de edad. Una vulnerabilidad del estatus legal de los menores, que en la legislación moderna se maneja como

doble vulnerabilidad, y el quebrantamiento de valores profundamente morales como la inocencia de la infancia, y la vulnerabilidad emocional de la adolescencia, sumada a un rechazo profundo por los delitos de corte sexual derivada de sus series impactos emocionales, su derecho a la indemnidad, en el caso de los niños específicamente; y al destrucción de principios morales y religiosos como la virtud o al inocencia, han dado un peso especialmente severo respecto de la persecución de estos delitos.

La pornografía como medio, es difícil de definir. Como explica Malem Seña (s.f) en términos legales, es difícil dar un significado único sobre la misma, explicando como esta es compleja de definir, aunque se identifica de manera inmediata al observarla. Sus raíces etimológicas, griegas cabe señalar, están la palabra Porneia, que vendría a significar adulterio o fornicación, aunque la pornografía moderna como moderna se alejado de su raíz griega, quedando únicamente un consenso general entre los doctrinarios que está se encuentra unida fundamentalmente a expresiones relacionadas a los genitales sexuales y a las relaciones íntimas en diferentes medios. Algunos autores como David Copp se refieren a ella como representaciones obscenas de órganos y comportamientos sexuales, que transgreden el decoro y los cánones de la decencia (p.1-2). Por su parte Morillas Fernández (2005) concuerda en la falta de unanimidad al darle una definición a lo pornográfico al referirse a la problemática específica de la pornografía infantil, señalando que la dificultad reside en la cantidad de observaciones que se deben delimitar. Este lo engloba dentro de explotación infantil, al cual designa como vocablo genérico que abarca la coacción del menor para la prostitución, su captación para el efecto, la práctica de actividades sexuales con un niño mediante coacción, fuerza o amenaza, y el uso de transacciones a cambio de estos servicios. Se define finalmente a la pornografía infantil como representación visual y real, con esto dejando fuera las simulaciones de edad, de un menor desarrollando actividades sexuales explicitas, explayando categorías con el fin de exponer el porqué de la persecución de una y la no persecución de otras.

Se exponen la pornografía infantil expresa, donde la representación tiene una participación explicita de un menor o niño, y la pornografía infantil simulada, que expresan situaciones en las cuales el supuesto menor no reúne las consideraciones de un menor por contar este con la mayoría de edad a pesar de su apariencia que derive en contrario o porque se trátase de un modelo producido por tecnología, y por tanto no se trátase de una persona real, siendo incapaz de adecuarse al tipo penal de pornografía infantil. Cabe señalar que esta interpretación entra conflicto con lo manejado

por la Convención. (p. 64-69).

4.3.4 Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Art. 10.- Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

1. Cada Parte adoptara las medias legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación de conformidad conas las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 2971, por la cual se revisó el Convenio de Berna para la protección de las Obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del tratado de la OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenio, cuando tales actos se cometan deliberadamente a escala comercial y por medio de un sistema informático

2. Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención internacional sobre la protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derecho s de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados

en los párrafos 1 y 2 del presente artículo. (Convenio sobre Cibercriminalidad, 2001, art. 10, p. 7)

La protección de los derechos de autor es ciertamente uno de los elementos de mayor importancia en la política y legislación delictiva digital ya que se puede argumentar que la distribución no autorizada y sin regulación de este contenido a través de foros y otras plataformas fue uno de los elementos fundamentales de un internet mucho más temprano. En este contexto, los Estados buscaron aplacar la susodicha problemática. Primero a través de su propia legislación, y posteriormente a través de la cooperación internacional a través de acuerdos o tratados advirtiendo el problema de territorialidad para poder perseguir dichos delitos realizados desde la distancia.

Art. 11.- Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo. (Convenio sobre Cibercriminalidad, 2001, art. 11, p. 8)

Lo cierto es que, la compleja naturaleza de los tipos penales en derecho informático ofrece grandes problemas al ponerlos a la prueba de fuego de la legislación. El derecho de propiedad intelectual ha encontrado un verdadero Goliat al tratar de enfrentarse a la piratería digital, debido en gran parte a que el internet es un ecosistema que por su naturaleza se resiste al control y la regulación, incluso hasta el día de hoy, por lo tanto, las facilidades para la piratería terminaban por entregar un espacio propicio para que grupos organizados de individuos con conocimientos informáticos buscaran tomar su pedazo del pastes, y sacar ganancia a partir de la reproducción ilegal de material sujeto a derechos de autor, ya fuera beneficiándose económicamente al vender versiones sin licencia del producto, aunque a un precio mucho más asequible gracias a no tener

que afrentar los costes de producción, o entregándolo a una comunidad de internet que cada vez veía la colaboración en foros, y la distribución de productos de libre licencia o de piratería digital, como un signo de colaboración y camaradería. La conformación de estos grupos, termino inevitablemente por desembocar en la formulación de leyes que tuvieran a la piratería informática en una apreciación igual a la de cualquier otro crimen, donde tanto la tentativa como la colaboración complicidad, respondían a legalmente frente a los perjuicios que están pretendían o llegaron a generar.

Art. 12.- Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de estas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;

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

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

2. Además de los casos previstos en el párrafo 1 del presente artículo, Cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito. (Convenio sobre Cibercriminalidad, 2001, art. 12, p. 8)

Así como las personas naturales encontraron formas de aprovecharse de las diferentes falencias en seguridad derivadas de la amplísima libertad que otorgaba el internet, así también lo hicieron personas jurídicas, y para sacarlo del contexto de la antigüedad, cabe mencionar que estas sigan haciéndolo hoy en día, a través de reclamaciones sobre creaciones originales de creadores de contenido independientes en internet, abusando de su tamaño o estatus. El modus operandí cambio, pero necesariamente el propósito. No obstante, el mejor ejemplo de una empresa abusando del internet y de los derechos de autor, y así mismo, de la aplicación de la responsabilidad penal de las personas jurídicas, es el caso del portal MEGAUPLOAD en 2012, el caso que puso en evidencia los avances de la legislación estadounidense en internet, su en forzamiento a través del Buró Federal de Investigación y una nueva tendencia en el intento de ponerle una figurada "correa de perro" al internet. El convenio establece una serie de pautas para la colaboración y manejo de una nomenclatura homogénea entre las naciones que los subscriben, sin embargo, el carácter de esta responsabilidad queda en manos de los Estados y por tanto su persecución no tiene un carácter homogéneo.

Art. 13.- Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12. (Convenio sobre Cibercriminalidad, 2001, art. 13, p. 8-9)

En concordancia con el punto anterior, al no tener una determinación homogénea respecto del tipo de responsabilidad que tienen las personas jurídicas, los términos de las sanciones quedan delegadas a los Estados, según determinara su legislación, aunque las acciones realizadas por la persona natural de manera equivoca tendrán un carácter sancionatorio penal, sea este en contravención o delito, pues la responsabilidad de la persona natural fue dejada en completa claridad tanto en su aplicación, como en la exclusiones.

4.4 Análisis jurídico de la Legislación penal ecuatoriana sobre derecho penal informático

El Código Orgánico Integral Penal, único y máximo cuerpo penal de la Republica del

Ecuador es un producto jurídico reciente. Su creación se remonta al 2014, fecha desde la cual se ha ido modificando gradualmente. Es decir, la ley penal ecuatoriana ha visto necesidad en reformarse y actuado en consecuencia, entre los ámbitos reformados, han sido incluidos ciertos tipos que se relacionan o tratan directamente delitos informáticos. A continuación, exploraremos estos tipos contenidos en sus respectivos articulados.

El derecho informático es una materia de relativa novedad. Lógicamente, los delitos informáticos siguen una línea similar. Si bien son una problemática difícil de tipificar, y de controlar, lo cierto es que ciertos delitos informáticos ya se encontraban vigentes antes de la promulgación del actual cuerpo penal en 2014, aunque con un enfoque inadecuado. Posterior a su vigencia, una serie delitos serían agregados en diferentes tandas por leyes reformatorias desde 2016, hasta 2022. Se tratarán por bloques para poder apreciar sus elementos comunes de manera homogénea.

> **Art. 103.-** Pornografía con utilización de niñas, niños o adolescentes. - La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual, aunque el material tenga su origen en el extranjero o sea desconocido, será sancionada con pena privativa de libertad de trece a dieciséis años.
>
> **Art. 104.-** Comercialización de pornografía con utilización de niñas, niños o adolescentes. - La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años. (Código Orgánico Integral Penal, 2014, art.103-104)

Identificándolos por sus elementos, siguiendo la Teoría del tipo penal, las conductas penalmente sancionadas son esencialmente la producción de representaciones sexuales de niños y menores de edad, con los procesos propios de la mismas; y el ejercicio de actividades comerciales con productos derivados de la primera respectivamente. El responsable en ambos escenarios es ambos tipos la o las personas que incurren en la conducta reprimida, configurándose además la antijuridicidad en el momento en que actúan contraviniendo la normativa, pudiendo por tanto imputársele el delito. La tipicidad será obviada en adelante pues el simple hecho de constar en

Código Orgánico Integral Penal la constituye.

En la legislación ecuatoriana, los delitos relacionados al contenido pornográfico tienen una estricta fijación sobre el tratamiento de los niños y menores de edad dentro de estos, estimando su posición de triple vulnerabilidad. Esto establece un punto, la pornografía, por si sola, no constituye un delito dentro del territorio ecuatoriano, ni su consumo de ningún tipo salvo las prohibiciones mencionadas, quedando regulado al ejercicio de las libertades al estipularse tanto la pornografía como su consumo como una actividad licita y legitima muy pesar de su reputación, interviniendo el mecanismo penal únicamente cuando hay vulneraciones sobre los derechos de aquellos quienes se consideran incapaces de poder tomar decisiones legales de peso debido a su incapacidad de asimilación como son los menores de edad y los niños. De estas prohibiciones se ven excluidos los interdictos y los ancianos en demencia, una situación que responde a no ser una parte sustancial en la industria ni un fenómeno recurrente, pero que no se puede pasar por alto como la ley ignora una protección para grupos que, por su estado mental, sufren características similares a las de los menores.

En este bloque se puede observar como el primer articulado, es decir el 133, actúa como prohibición madre, siendo el 104 un artículo auxiliar, que no implica que no sea un tipo independiente, pero que al encadenarse en la misma secuencia lógica de un acto, es decir el producir el material prohibido, y distribuirlo, funciona como un mecanismo para poder atribuir responsabilidad a cada parte de la cadena de acción independientemente de su involucramiento en la conducta reprimida originaria, la producción de pornografía, pudiendo de este modo ser imputados penalmente quienes auxilien en el comercio de este material, que lógicamente es prohibido al ser el producto de una actividad suprimida por la ley, a la vez que aporta un serie de condicionantes para poder ejercer el examen de los hechos al momento de determinar el tipo de concurso sobre el cual responderán, ya que al ser acciones conexas, determinar la dependencia de la primera acción, la de producir, con la segunda, la comercializar, será clave para determinar si corresponde el concurso ideal o el concurso real de delitos.

Lógicamente, debido al contexto de intercambio de información y contenido masivo que derivo de la internet, la legislación comprendió adecuadamente como esta podría ser usada fácilmente para poder distribuir contenido pornográfico relacionado con menores. Por tanto, los delitos relacionados con la pornografía con menores de edad tienen primero un carácter sexual, es decir, siguen las observaciones de los delitos contra la sexualidad, y segundo, un carácter

informático que fue heredado y forjado por la circunstancia del modus operandi de este comportamiento delictivo.

> **Art. 154.1.- Instigación al suicidio. -** Será sancionada con pena privativa de la libertad de uno a tres años, la persona que induzca o dirija, mediante amenazas, consejos, órdenes concretas, retos, por medio de cualquier tipo de comunicación verbal, física, digital o electrónica existente, a una persona a que se provoque daño así mismo o ponga fin a su vida, siempre que resulte demostrable que dicha influencia fue determinante en el resultado dañoso.
>
> **Art. 154.2.- Hostigamiento. -** La persona natural o jurídica que, por sí misma o por terceros o a través de cualquier medio tecnológico o digital, moleste, perturbe o angustie de forma insistente o reiterada a otra, será sancionada con una pena privativa de la libertad de seis meses a un año, siempre que el sujeto activo de la infracción busque cercanía con la víctima para poder causarle daño a su integridad física o sexual.
>
> Cuando la víctima sea menor de dieciocho años de edad, o persona con discapacidad o cuando la persona no pueda comprender el significado del hecho o por cualquier causa no pueda resistirlo, será sancionada con pena privativa de libertad de uno a tres años.
>
> **Art. 154.3.- Contravenciones de acoso escolar y académico. -**
>
> 1. Acoso académico: Se entiende por acoso académico a toda conducta negativa, intencional, metódica y sistemática de agresión, intimidación, ridiculización, difamación, coacción, aislamiento deliberado, amenaza, incitación a la violencia, hostigamiento o cualquier forma de maltrato psicológico, verbal, físico que, de forma directa o indirecta, dentro o fuera del establecimiento educativo, se dé por parte de un docente, autoridad o con quienes la víctima o víctimas mantiene una relación de poder asimétrica que, en forma individual o colectiva, atenten en contra de una o varias personas, por cualquier medio incluyendo a través de las tecnologías de la información y comunicación. (Código Orgánico Integral Penal, 2014, art.154.1; 154.2; 154.3)

Los elementos del tipo correspondientes a este grupo tienen una clara conducta común como elemento en términos generales, los aspectos derivativos responden a su modalidad, que es el hostigamiento del individuo, entendiéndose entonces como responsable, todo aquel que cometa

estas infracciones, diferenciándose los tipos por la gravedad del acto, o del producto del mismo, pudiendo ser mero hostigamiento, o este concluir en muerte. También se diferencia por la relación de poder entre la víctima y el imputado. La antijuridicidad se solidifica sobre la base de la violación no solamente de la norma penal, sino por contravenir disposiciones constitucionales como el derecho a la vida, salud y buen vivir.

El nuevo contexto digital significo a su vez, un nuevo contexto para el uso y abuso del poder que tiene un individuo sobre otro, y de las amenazas, en especial las anónimas, las cuales se volvieron pan de cada día. Es por esta razón, que, a través de varias reformas la Asamblea fue reformando el Articulo 154.

Este artículo, se refiere sobre la intimidación, es decir, el acto de amenazar con una la realización de un hecho ilegal que, acompañado del contexto que permita determinar que la amenaza es plausible, tiene como consecuencia de la desobediencia del sujeto pasivo.

Todos los tipos aquí englobados, tienen por característica común, el derivarse de actos lesivos de carácter verbal, sean estas amenazas, intrusiones por correspondencia o abuso verbal que culminan con la perturbación de la tranquilidad y paz del individuo en primera instancia, pudiendo degenerarse en consecuencias con mayor gravedad.

Esta naturaleza verbal hace que la informática entre en juego, esto debido a que nuestro día la gran mayoría de los intercambios de información verbal significativa se da dentro de un ecosistema cibernético y como tal, contextualiza estos delitos dentro de los delitos informáticos.

Art. 166.- Acoso sexual. –

Inciso segundo: Se considerará ciberacoso sexual cuando la conducta descrita en el inciso anterior se realice utilizando cualquiera de las tecnologías de la información y comunicación, medios tecnológicos, electrónicos o digitales, y será sancionado con una pena privativa de libertad de uno a cinco años.

Art. 170.- Abuso sexual. –

Inciso cuarto: Se sancionará con el máximo de las penas establecidas en los incisos precedentes, cuando dicho abuso sexual fuese grabado o transmitido en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación.

Inciso quinto: Asimismo, el máximo de las penas establecidas en los incisos precedentes, cuando además de la grabación o transmisión de este abuso sexual con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, se agreda físicamente a la víctima, y dicha agresión también sea grabada o transmitida.

Art. 171.- Violación. –

6. Cuando dicha violación es grabada o transmitida en vivo de manera intencional por la persona agresora, por cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación.

7. Cuando además de la grabación o transmisión de esta violación con cualquier medio digital, dispositivo electrónico o a través de cualquiera de las tecnologías de la información y comunicación, se agreda físicamente a la víctima, y dicha agresión también sea grabada o transmitida. (Código Orgánico Integral Penal, 2014, art. 166, art. 170, art. 171)

Las conductas gravadas son en términos generales transgresiones a la integridad sexual de la víctima, realizándose una diferenciación de tipos según su gravedad o modo con el fin de poder hacer un uso efectivo del principio de proporcionalidad en la formulación sobre la gravedad de la sanción, quedando la antijuridicidad en la violación de la prohibición, siendo así el acto incompatible a su vez con postulados constitucionales como la privacidad, salud y buen vivir.

Los delitos anteriormente abarcados no son informáticos puros. Nuevamente, son primero delitos en contra de la integridad sexual y reproductiva, los medios informáticos no son sino un medio para la consolidación del acto. No obstante, debido a las redes sociales, el modus operandi de muchos sujetos criminales integro el uso de estas como medios para la comisión de los delitos, puesto que ofrecen facilidades relacionadas a información personal, horarios, personas cercanas, residencia o lugares frecuentados; sumado al propio anonimato. Es decir, nociones que para, por ejemplo, predadores sexuales, son de gran utilidad. Por tanto, los delitos antes mencionados adquirieron por necesidad y contexto un carácter informático, primero de facto, y luego a través de la adhesión de numerales que establecían el involucramiento de dispositivos telemáticos, electrónicos o de tecnologías de la información.

Contextualizada adecuadamente la situación relacionada a estos delitos, prosigue el observar y analizar sobre los comportamientos descritos, los cuales evidencian una consciencia

sobre el uso de los medios informáticos para la divulgación de material sexual sin consentimiento de las víctimas. Los llamados packs son ejemplo de este comportamiento que, por su difícil persecución por parte de los afectados, se convirtió en uno de incidencia considerablemente alta.

Estos en conjunto con los demás comportamientos que se pudieran derivar de la exposición a través de medios informáticos se configuran como agravantes constitutivos de estas acciones, pues no solo se evidencia un dolo intrínseco en la acción, sino también un intento activo por despojar de la dignidad, la intimidad y la honra a la otra persona.

> **Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos. -** La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.
>
> Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.
>
> La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.
>
> **Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. -** La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años. (Código Orgánico Integral Penal, 2014, art.173-174)

Los Artículos 173 y 174, al igual que los relacionados con la pornografía infantil, toman su accionar reprimible penalmente del involucramiento de los menores o niños, es decir, el bien jurídico tutelado sigue siendo la integridad sexual y reproductiva, pero se enfatiza una categoría diferente al ser los menores beneficiarios del estado de doble vulneración, al considerarse aun incapaces jurídicamente de tomar sus propias decisiones.

Debido a que las comunidades de pedófilos tomaron la falta de regulación de la red como

una ventaja singular a explotar, es que se forjaron estos tipos, los cuales en su contenido imponen represión sobre el acercamiento sobre los menores e infantes, nuevamente contemplando su triple vulnerabilidad, al momento de velar por su protección.

El primer de estos dos, tipifica el llamado Grooming, que es en palabras cortas, personas adultas acercándose a través de cuentas de usuario falsas, y por tanto a través del engaño actuando así dolosamente, a menores o infantes con finalidades sexuales. Por otro lado, el segundo, se alinea más en los términos de la explotación de estos niños y menores, ambos compartiendo en común la predilección del modus operandi de estos delitos a través de medios informáticos y tecnologías de la información.

> **Art. 178.- Violación a la intimidad. -** La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.
>
> **Art. 179.- Revelación de secreto o información personal de terceros. –** La persona que teniendo conocimiento por razón su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación cause daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año. No habrá delito en aquellos casos en que el secreto divulgado verse sobre asuntos de interés público.
>
> Sera sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenidos digitales, mensaje, correos, imágenes, audios o videos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad. (Código Orgánico Integral Penal, 2014, art.178-179)

Estos delitos tienen como característica en común el estar vinculados con la intimidad, el secreto y la información personal con su manejo.

Dentro de la legislación penal ecuatoriana se contempla como violación de la intimidad a la difusión, acceso o manejo de información privada del sujeto pasivo, que puede ser tan solo uno o más en caso de que se acceda de esta manera a la información de un tercero, sin su consentimiento, entendiéndolo siempre desde la informática y las telecomunicaciones, las cuales

son elementos constitutivos de este tipo penal.

El Artículo 179, por otra parte, es un delito independiente de los medios informáticos, esta principalmente direccionado a garantizar el correcto desempeño del secreto profesional. No obstante, su segundo inciso atiende sobre la distribución de esta información a través de estos medios que, si bien no lo vuelven un delito informático por naturaleza propia, lo enmarcan dentro del campo informático, entendiendo que esta provisión de agravio constituyente deriva del impacto potencial que tiene la publicación de información personal protegida por el secreto, en medios de comunicación masiva y alta accesibilidad.

> **Art. 186.- Estafa. -** La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. (Código Orgánico Integral Penal, 2014, art.186)

La Estafa es una muestra de la tendencia qué existe en los tipos penales, de involucrarse con tecnologías de la información y medios adjuntos, esto con el objetivo de ganar mecanismos operacionales, y de aprovecharse del precario conocimiento y consciencia con la cual la población general navega en la web. Misma que explotan para, a través de ingenuidad e inocencia de los usuarios, engañarlos a través de mensajes que suplantan familiares, venta de productos ficticios, o la promoción de esquemas piramidales fraudulentos. Aunque el tipo penal ecuatoriano no caracteriza el uso de medio informáticos como un apartado dentro de su descripción del tipo. Bajo esto entendemos que lo abarca por generalidad, no obstante, y por tanto lo entendemos como un delito involucrado en la delincuencia informática debido a la creciente incidencia del uso de la TIC para su cometimiento, lo que ha derivado en la estafa adquiriendo un peso importante dentro de los delitos informáticos, por ser un modus fundamental, pues buena parte de los delitos informáticos se manejan a través del engaño, la suplantación y la manipulación de la información; y viceversa, ya que gran parte de las actividades de Estafa son profundamente dependientes del uso los mencionados medios.

> **Art. 190.- Apropiación fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transparencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra

persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretad o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridad electrónicas, informáticas u otras semejantes.

(Código Orgánico Integral Penal, 2014, art.190)

La apropiación fraudulenta tipifica una actividad que requiere de la existencia de medios informáticos para su desarrollo. Tipifica como sancionable de uno a tres años, al hecho de tratar de hacerse con el control de un bien ajeno, a través del uso fraudulento de software. El comportamiento descrito puede acoplarse al irrumpir forzosamente sobre una base de datos del estado, y cambiar valores de la titularidad, por poner un ejemplo. Además de esto, contempla en igual valor a quien no haga su entrada de manera forzosa en el sistema, pero si a través de medios sin autorización, como puede ser, captar la clave de una cuenta y entrar con esta.

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles. - La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles. - La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 195.- Infraestructura ilícita. - La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal, 2014, art.191,192,195)

Los artículos antes señalados, sumado al artículo 190, están todos englobados dentro de los delitos en contra de la propiedad dentro del Código Orgánico Integral Penal. Estos delitos

atentan contra la posesión y la titularidad de un objeto sujeto de derechos de propiedad. En este escenario en particular, la titularidad de erosiona por medios informáticos, tales como la reprogramación de un equipo, que busca volverlo inidentificable para el propietario por medio de los datos del dispositivo; la venta y reventa de la información relacionada con estos datos de identificación, exponiendo así la información del dispositivo para posible ataque al mismo posterior y por último el uso de la infraestructura ilícita, cuya actividad sancionada actúa como soporte del resto, actuando como una estructura para el cometimiento de delitos, volviéndose de suma importancia el suprimir no solo las actividades penales individualizadas, sino también a la raíz que es la infraestructura que permite su subsistencia prolongada y a cambio del beneficio económico de quien la desarrolla.

Art. 208A.- Actos lesivos a la propiedad intelectual. – Será sancionada con pena privativa de libertad de seis meses a un año, comiso y multa de ocho hasta trescientos salarios básicos unificados del trabajador en general, la persona que, a sabiendas, en violación de los derechos de la propiedad intelectual contemplados en la normativa aplicable, realice uno o más de los siguientes actos con fines de lucro y a escala comercial

(…)

4. Almacene, fabrique, utilice, oferte en venta, venda, importe o exporte:

(…)

f) Un producto o servicio que utilice un signo distintivo no registrado idéntico o similar a un signo distintivo registrado en el país; y

g) Un producto o servicio que utilice un signo distintivo o denominación de origen no registrada, idéntica o similar a una denominación de origen registrada en el país.

En los casos de los literales f) y g) de este cuarto numeral los productos o servicios que utilicen el signo no registrado deberán ser idénticos o que guarden conexión competitiva a los productos o servicios protegidos por las marcas o indicaciones geográficas registradas en el país.

Art. 208B.- Actos lesivos a los derechos de autor. - Será sancionada con pena privativa de libertad de seis meses a un año, comiso y multa de ocho hasta trescientos salarios básicos unificados del trabajador en general, la persona que, a sabiendas, en violación de los derechos de autor o derechos conexos contemplados en la normativa aplicable, realice uno o más de los siguientes actos a escala comercial:

a) Altere o mutile una obra, inclusive a través de la remoción o alteración de información electrónica sobre el régimen de derechos aplicables;

b) Inscriba, publique, distribuya, comunique o reproduzca, total o parcialmente, una obra ajena como si fuera propia;

c) Reproduzca una obra sin autorización del titular o en un número mayor de ejemplares del autorizado por el titular, siempre que el perjuicio económico causado al titular sea mayor a cincuenta salarios básicos unificados del trabajador en general;

d) Comunique públicamente obras o fonogramas, total o parcialmente;

e) Introduzca al país, almacene, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceras reproducciones ilícitas de obras o en número que exceda del autorizado por el titular;

f) Reproduzca un fonograma o en general cualquier obra protegida, así como las actuaciones de intérpretes o ejecutantes, total o parcialmente, imitando o no las características externas del original, así como quien introduzca al país, almacene, distribuya, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceros tales reproducciones ilícitas;

g) Retransmita sin autorización, por cualquier medio, las emisiones de radiodifusión, televisión y en general cualquier señal que se transmita por el espectro radioeléctrico y que esté protegida por derechos de autor o derechos conexos; salvo que dicha retransmisión provenga de una obligación normativamente impuesta; y,

h) Fabrique, importe, exporte, venda, arriende o de cualquier forma distribuya al público un dispositivo, sistema o software que permita descifrar una señal de satélite cifrada portadora de programas o en general de telecomunicaciones, sin autorización del

distribuidor legítimo de esa señal; o, de cualquier forma, eluda, evada, inutilice o suprima un dispositivo, sistema o software que permita a los titulares del derecho controlar la utilización de sus obras o prestaciones, el cual posibilite impedir o restringir cualquier uso no autorizado de estos. (Código Orgánico Integral Penal, 2014, art.208A-208B)

Como fue explicado con anterioridad en el estudio de la doctrina. El derecho de propiedad intelectual y los derechos de autor son de los principales elementos a los cuales el derecho informático respondió. Estafas y piratería era lo que abundaba en la red en su temprano desarrollo, y, por tanto, se requería un accionar consecuentemente por parte de la legislación para poder para estos actos delictivos.

La legislación para determinar la lesividad de las acciones en contra de delitos relacionados al derecho de propiedad intelectual y de autor han existido con anterioridad en el Ecuador. Dentro del Código Orgánico Integral Penal se incorporó a través de reformas, una primera en 2015 y otra ultima en 2021, que es la que da origen a los dos artículos anteriores.

En primera instancia, cuando se promulgo, el Código Orgánico Integral Penal no contemplaba este delito, ni artículos que regularan esta conducta. Esto cambio con el pasar de los años, y la última reforma, la 2021, remplazando el único artículo que abarcaba, en términos muy generales, la falsificación y la piratería lesiva. Se agregaron muchos más términos respecto de las acciones que se consideraban lesivas, y se hizo una diferenciación en función de la propiedad intelectual y el derecho de autor, entendiendo que el primero y matriz de estos, regula respecto estrictamente a las ideas que configuran una expresión artística, literaria o científica, es decir la configuración formal de la idea; mientras el segundo, son derechos que se derivan respecto de la propiedad de la idea. La separación es importante, porque la lesión a la titularidad de una idea no tiene la misma intención o motivo que la lesión sobre los derechos que tiene el autor sobre la misma. Por poner un ejemplo, existe diferencia entre que yo reproduzca sin autorización una idea, que es un derecho que tiene su creador, al hecho de que trate de usurpar su titularidad, lo cual a su vez significa arrebatar todos los derechos derivados de la misma.

Actualmente, por estos artículos, se encuentran sancionados penalmente las acciones que lesionen la propiedad intelectual y sus derechos derivados, estimándolos como procesos diferentes por las consecuencias jurídicas diferentes que tienen como consecuencia.

Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.

2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.

3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.

4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (Código Orgánico Integral Penal, 2014, art.230)

Este artículo fue modificado por reforma en 2021, agregándose un numeral y añadiendo el carácter ilegitimo al numeral dos que se refiere respecto de los intentos de inducir al usuario a entrar a una dirección que este no desea, esto a través del engaño.

Art. 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.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo

patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, sistemas de tecnologías de la información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 233.- Delitos contra la información pública reservada legalmente. - La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.

2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Art. 234.1.- Falsificación informática:

1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.

2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena. (Código Orgánico Integral Penal, 2014, art. 231-234.1)

Estos artículos, incluido el 230, tipifican varias actividades que son comunes en la ciberdelincuencia para la configuración de muchos de sus ataques estándar como lo son la irrupción en canales privados sin autorización, el fishing, el craking y otros comportamientos derivados.

Art. 234.2.- Agravación de las penas. - La práctica de los hechos que se describen en los artículos 232, 234 y 234.1 será sancionada con pena agravada en un tercio de su pena máxima si logra perturbar de forma grave o duradera a un sistema informático que apoye una actividad destinada a asegurar funciones sociales críticas, como cadenas de abastecimiento, salud, seguridad y bienestar económico de las personas, o funcionamiento regular de los servicios públicos.

4.5 Derecho Comparado

4.5.1 Legislación española: Código Penal Español

La legislación española es por cuestiones relativas a la naturaleza de su estado y su sociedad, la más ajena de las legislaciones a comparar. La adaptación de los estados europeos a la tecnología, el ser parte del Consejo de Europa, órgano que redacto la Convención de Ciberdelincuencia, y la Unión Europea, que, en su esfuerzo por configurar una unión aduanera, impuso una temprana valoración de la protección de los derechos de autor y patentes, ha contribuido a que la legislación penal en el Reino de España se encuentre más acorde con las expresiones esperadas del primer mundo, que de la órbita hispanoparlante.

Los primeros delitos a introducir están enmarcados dentro del Título V: Delitos contra la Libertad Sexual. Son delitos que dentro de la ley española son lesivos en contra de la el bien jurídico de la sexualidad. El componente informático en esta deriva de la captación y la distribución a través de medios informáticos como elemento común. Como se mencionó antes, estos son delitos sexuales primero, y delitos informáticos segundo, comprendiendo que existe una jerarquía en el agravio que estos producen, sin por esto, descalificarlos en ningún momento como delitos informáticos. Después de todo, la propia Convención para la Cibercriminalidad la estima de igual manera.

La legislación penal española respecto de los delitos informáticos encuentra recogida en su totalidad en el Código Penal de 1996, emitido por Cortes Generales. Estos tipos no se encuentran recogidos en un solo apartado, estando dispersos en el código, seguramente como consecuencia de haberse incorporado reforma a reforma.

Artículo 183

> 1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

Dentro de la legislación española, el gromming, es decir el contactarse con un menor de dieciséis a través de medios informáticos, con el fin de acordar un encuentro que terminase en estupro y demás conductas sexuales, o con el fin de exponer pública o privadamente; capturar a través de fotografía o video actos sexuales que involucren menores de dieciséis, entendiendo esta última como pornografía infantil. Sin embargo, aquí el acto punible no está en las consecuencias, estas si se concretan serán las que determinen otros tipos penales como el estupro, o como veremos más adelante, la pornografía infantil. No, aquí el agravio se encuentra en el accionar material de hacer preparativos para concertar un acto sexual con un menor, es decir haber creado de manera voluntaria y premeditada las condiciones para la sucesión del acto sexual; y el uso del engaño, la manipulación y hasta una posición de poder, para inducir a un menor para entregar imágenes pornográficas que representen partes de su cuerpo desnudo o semidesnudo. Esto atendiendo siempre que la inducción al error vicia por completo el consentimiento y por lo tanto este no se puede argumentar.

Por su parte, la legislación ecuatoriana cuenta con dos artículos que atiende al accionar particular de acercarse a alguien con intenciones sexuales. Este vendría a ser el Artículo. 173 del Cogido Orgánico Integral Penal, que lleva por nombre Contacto con menores de dieciocho años por medios electrónicos, La legislación ecuatoriana se diferencia de la española en dos puntos a señalar.

El primero, la edad que abarca el tipo. Mientras que la legislación española es más laxa respecto de la edad hasta la cual se protege a los jóvenes de este tipo de acercamientos, situando la edad contemplada en el tipo en los dieciséis años; la legislación ecuatoriana toma una postura de protección sobre toda persona que no sea mayor de edad.

El segundo se corresponde con la búsqueda de obtener o mostrar material pornográfico a menores por medios tecnológicos. El art. 173 del Código Orgánico Integral Penal se centra en tipificar el acercamiento a través del engaño, y el agravante de la fuerza, quedando este acercamiento recogido por otros dos artículos: el 166, del acoso sexual, en su inciso segundo sobre

el ciberacoso; y el 169, de la corrupción de niñas y adolescentes, aunque este último carece de una contemplación respecto del uso de dispositivos tecnológicos o a su realización través de estos.

Esto dice el Art. 189 que determina las condiciones específicas sobre los resultados del numeral dos del artículo anterior.

Artículo 189

1. Será castigado con la pena de prisión de uno a cinco años:

(…)

b) El que produjere, vendiere, distribuyere, exhibiere, ofreciere o facilitare la producción, venta, difusión o exhibición por cualquier medio de pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección, o lo poseyere para estos fines, aunque el material tuviere su origen en el extranjero o fuere desconocido.

A los efectos de este Título se considera pornografía infantil o en cuya elaboración hayan sido utilizadas personas con discapacidad necesitadas de especial protección:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad necesitada de especial protección participando en una conducta sexualmente explícita, real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad necesitada de especial protección con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales.

(…)

5. El que para su propio uso adquiera o posea pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, será castigado con la pena de tres meses a un año de prisión o con multa de seis meses a dos años.

La misma pena se impondrá a quien acceda a sabiendas a pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección, por medio de las tecnologías de la información y la comunicación.

(…)

8. Los jueces y tribunales ordenarán la adopción de las medidas necesarias para la retirada de las páginas web o aplicaciones de internet que contengan o difundan pornografía infantil o en cuya elaboración se hubieran utilizado personas con discapacidad necesitadas de especial protección o, en su caso, para bloquear el acceso a las mismas a los usuarios de Internet que se encuentren en territorio español.

En el texto penal español, se establece a través de este articulado la sanción sobre actividades que estén encaminadas a la subsistencia de la pornografía infantil. Hablamos de acto, captación en video o cualquier otro medio, y oferta a través de medios físicos o virtuales. Esto desde la parte que lo genera, mientras que por otro lado se hace una diferenciación con la persona que posea esta clase de contenido, aunque teniendo una reprimenda menor a la del primero.

Como puntos principales a señalar sobre el tratamiento de la legislación penal española sobre esta temática se encuentra en su diferenciación clara sobre las características que conforman la figura de la pornografía infantil. Mientras que la legislación ecuatoriana hace una identificación de los elementos que configuran de manera breve y general. Una definición que puede ser cuestionada seriamente cuando se somete la representación artística; y una herramienta por la cual se han valido múltiples representaciones de desnudos de menores de edad, como lo pueden ser obras antiguas; y que sin embargo ha logrado que ciertas obras con trasfondo claramente erótico, hayan encontrado protección en este concepto artísticas, como pueden presentar obras como el hentai o de géneros pornográficos que buscan simular a través de personas con un desarrollo físico escaso como es el petite. Puede ser por esto que la legislación española esmero en delimitar tanto como fuera legalmente posible las situaciones sobre las cuales podía sopesar este tipo penal, dejándolo de este modo fuera de la posibilidad de la interpretación artística o sobre la relatividad

de la apariencia y la edad.

Agregado a esto el artículo 189 tiene plena consciencia del valor que tienen las redes informáticas y demás medios tecnológicos relacionados para el desarrollo moderno de esta actividad delictiva. Desde la creación, pasando por el almacenamiento y finalmente la distribución efectiva del producto. Sumado a esto, es consciente que la ley debe ser, además de sancionadora, reparativa, concentrándose principalmente en la no repetición. Motivo por el cual se establece obligación de los jueces y tribunales para tomar las medidas necesarias para poder retirar el contenido en cuestión, y el desmonte de los sitios donde estos se suban, entendiendo que la sobre ellos recae responsabilidad sobre la moderación de los contenidos; o volviéndolos inaccesibles desde las fronteras del Reino. La ley también faculta la aplicación de estos efectos de manera cautelar, entendiendo que siempre sobre este tipo de delitos, los sujetos pasivos son menores y niños, que son sujetos de triple vulneración, y por tanto deben tener una serie de protecciones especiales. En este caso, la protección está en la inhabilitación del acceso efectivo al material lesivo contra su sexualidad, o que puede ser declarado potencialmente afectivo. La legislación ecuatoriana no tiene ninguno de estos aspectos específicos encontrados en la ley española. Si bien existe el tipo, como se mencionó anteriormente, este se dedica a tipificar la mera acción, sin delimitar claramente sus límites, limitándose a establecer en dos tipos separados responsabilidad sobre la tenencia, y comercialización. No se delimita los límites de las expresiones pornográficas, lo cual es un fallo ya que se desestima totalmente la ambigüedad visual del desarrollo físico con la edad. Tampoco se mandan procesos de intervención de la justicia para dar de baja el material, dejando los términos sobre el cómo se va a reparar los daños derivados de estos delitos a los mecanismos generales de reparación integral que se establecen en el Artículo 78 del Código Orgánico Integral Penal, especialmente la Garantía de no Repetición.

Artículo 189 bis

> La distribución o difusión pública a través de Internet, del teléfono o de cualquier otra tecnología de la información o de la comunicación de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II bis y IV del presente título será castigada con la pena de multa de seis a doce meses o pena de prisión de uno a tres años.

> Las autoridades judiciales ordenarán la adopción de las medidas necesarias para la retirada de los contenidos a los que se refiere el párrafo anterior, para la interrupción de los servicios que ofrezcan predominantemente dichos contenidos o para el bloqueo de unos y otros cuando radiquen en el extranjero.

Este artículo, en una línea similar a los anteriores, tiene plena consciencia de la influencia que tiene la informática, la tecnología y los medios de comunicación masivos como mecanismos de organización, extensión de ideas, comercio y distribución. Un solo recuso digital, véase un video ligado a una URL, puede reproducirse masivamente sin control dentro de las redes, suponiendo un grave daño a la integridad sexual cuando esto sucede. Agregado a esto, está la propiedad se servir como portal de oferta de servicios sexuales con menores, actuando como intermediario. Estos factores son importantes para entender el por qué se requirió de un artículo reformatorio que contemplara la difusión redes, ya que estas pueden tener un efecto severo en la integridad sexual derivado de la capacidad de replicación y su difícil control de contenido.

No obstante, si bien se puede argumentar que quien ofrece, alienta; existen diferencias al entender la posición de ambas legislaturas. Ambas legislaciones suprimen un acto que busca activamente ofrecer un servicio, y, por tanto, la facilitación de mecanismos y medios para la comisión de otros delitos sexuales en contra de los menores. No obstante, existe una apreciación diferente respecto de la gravedad del acto en ambas legislaciones. La ecuatoriana es mucho más severa e impone una pena privativa de la libertad que ronda desde siete a diez años. Por su parte, la legislación española contempla una pena desde uno a tres años.

Esta diferencia en la apreciación de la gravedad probablemente se deba a que, para la legislación española, este delito destaca un comportamiento de intermediario, en el cual es sujeto activo es una conexión con material que puede ser de autor externo, o con otros individuos que poseen los recursos o los medios para la comisión de actividades sexuales punibles. Por otra parte, para la legislación ecuatoriana, el sujeto activo no actúa como un intermediario con un proveedor de servicios, el sujeto activo es en sí el proveedor de servicios, ya que la ley menciona claramente que se sancionara el uso de medios electrónicos, telemáticos o tecnológicos para ofrecer servicios con menores de edad, siendo la palabra con el elemento más importante del enunciado, ya que establece una conexión directa con el menor para el acto sexual. Donde en la legislación española el sujeto activo es un intermediario para conseguir desde material pornográfico, hasta medios para que otra persona pudiera cometer el delito sexual; la legislación ecuatoriana tiene por sujeto activo

a un individuo que ofrece un servicio con un menor. No pornografía conseguida de fuente desconocida, no videos que simulan el acto, no medios indirectos para que otra persona pueda concertar el delito. Él es el proveedor, y por lo tanto controla de algún modo la posición del sujeto pasivo en una relación de autoridad o amo, de la cual saca provecho a través de ofrecerlo en servicio a terceros, similar al rol que toma un proxeneta.

Artículo 197.

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

(…)

Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.

> Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada.

La ley española tipifica en un solo artículo la captación y la revelación de datos ilegalmente. La legislación emitida por las cortes es una que regula el carácter general de ambos aspectos mencionados anteriormente, estableciendo diferentes escenarios para la obtención de estos, siendo el escenario informático uno de estos. Aunque no se encuentre descrito técnicamente en el primer numeral de este artículo, lo cierto es que la intercepción de correos electrónicos, que son mensajes de datos, es por su naturaleza un acto informático, pues la única manera de acceder a la base de datos donde estos se encuentran es a través de un medio como tal, sumado a que la intervención en las telecomunicaciones es una definición amplia que puede abordar además un escenario informático.

El segundo por su parte es taxativo en la relación con la informática, estableciendo que la pena, una de uno a cuatro años, será equivalente en el caso de acceder a información que se encuentre almacenada en una base de datos sin autorización, sean estos registro públicos o privados. Haciendo una equivalencia entre el acceso, en su última línea; la alteración, la adquisición y el uso de los datos mal habidos.

La ley ecuatoriana trata los elementos de estos numerales en el Art. 230 el cual lleva por nombre Intercepción ilegal de los datos, siendo un artículo estrictamente informático. El artículo en la norma penal española desarrolla un tipo amplio. Está expone sujetos activos con verbos rectores varios, y que responden a diferentes sanciones según los distintos escenarios que se haya descrito en sus numerales, siendo el uso de medios informáticos, un elemento que existe en algunos de estos escenarios, mas no en todos. Por otro lado, en la legislación ecuatoriana el componente informático es un elemento constitutivo del delito, indispensable, por lo tanto, y como tal desarrolla un tipo de exponer tres roles diferentes en la intercepción que responden a una pena equivalente, una de uno a cinco años. Estos roles se podrían definir como quien capta, quien provea medios y quien ejecute e infecte. El primero sanciona a la persona que se introduce a la fuente donde se encuentre almacenada la información en cuestión, este acceso puede hacerse a través de verbos varios, pero el elemento fundamental es que el sujeto haya captado información de un sistema informático sin autorización. El segundo describe la acción de un sujeto primero, para dar medios, puedan ser estos en software o contraseñas, para el cometimiento del delito, entiendo que estos

fueron dados o ideados con este propósito en mente. El tercero sanciona un sujeto consecuente del numeral dos, es decir, quien haga uso de los medios proveídos en software para instalarlos en un equipo, con el fin de configurarse la captación de la información. Este último tipo esta especialmente relacionado con el uso de spyware, worms y otros tipos de malware captadores de información. Los últimos dos numerales describen roles derivados de los últimos dos descritos, pero relacionadas tarjetas con banda magnética, una modalidad dentro de la informática, pero que es un producto de tiempos más tempranos de la ciberdelincuencia.

El tercer numeral español sanciona en contra de la relevación o cesión de datos producto de los dos anteriores numerales, entendiendo que esta es una ampliación del actuar del sujeto activo, y por lo tanto agravando la pena consecuente, pasando a la privación de dos a cinco años. En el Ecuador la revelación de estos datos estaría enmarcado dentro del artículo 229, describiendo la acción de revelar los datos extraídos de una base de datos, teniendo una pena más indulgente que la española para este accionar, siendo esta de uno a tres años. Existe también el Art. 179 cuya descripción de los actos es muy similar, sin embargo, la violación de la intimidad no requiere del provecho necesariamente para configurarse.

Artículo 197 bis.

1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

La legislación penal española determina el ingreso no consentido de un individuo al sistema informático de otra persona, a través de vulnerar la seguridad de este. Debido al requisito de una alta capacitación que caracteriza a este tipo de actividades delictivas, la posibilidad de conseguir acceder a un sistema de manera no intencionada es altamente improbable. Por tanto, el carácter del

delito se explica como doloso cuando se expone que se requiere la vulneración del sistema de seguridad, pues deberá ser un acto que busque activamente superar las medidas de seguridad formuladas para el efecto, demostrando un comportamiento antijuridico premeditado.

El segundo numeral se refiere respecto de únicamente la acción de interceptar, lo que no implica necesariamente la irrupción de alguna barrera de seguridad, al menos no expresamente, pero por la descripción su vulneración queda sugerida implícitamente, ya que se declara que el accionar debe ser sin autorización con el uso de artificio o instrumento técnico, es decir se establece la necesidad poseer capacidades técnicas para irrumpir a través de un sistema que de otro modo sería inaccesible. Este accionar dentro de la legislación ecuatoriana se encuentra contenido en el Art. 234 que establece la ilegalidad de acceder a un sistema informático, telemático o de telecomunicaciones sin consentimiento. Al igual que en la ley española, la actividad actúa sin consentimiento, y requiere la estancia prolongada dentro del mismo. Aunque la legislación ecuatoriana es más severa en cuanto a la condena correspondiente, siendo esta de 3 a 5 años, superior a la española de 1 a 4 años.

Artículo 197 ter

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información

Este articulo hace una apreciación selectiva sobre los delitos desarrollados exclusivamente en los dos artículos anteriores a este. Es decir, su efecto se encuentra claramente limitado a los términos que se establecieron en estos artículos, tiene efecto en los términos de este. No así, la legislación ecuatoriana que en Art. 230. Numeral 2, 3 y el 232 inciso 2 en las cuales se sancionan respecto del desarrollo de programas con el fin de secuestrar, alterar, captar o dañar un sistema informático ajeno, con pena de tres a cinco años, mientras que la ley española contempla de seis meses a dos años.

Artículo 197 quater.

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

La contemplación de la organización criminal contextualizada por la progresiva adopción de estas respecto de los mecanismos delictivos que provee el fenómeno de la ciberdelincuencia han resultado como consecuencia en la inclusión de este apartado dentro de la ley española. La caracterización de este accionar como un agravante es consecuente con el concepto de dolo, la premeditación y el concurso de roles, ya que las organizaciones criminales se configuran con el propósito de causar acciones antijuridicas, en beneficio propio, y con una asignación de roles en una jerarquía organizada para de esta manera garantizar a través de la mayor cantidad de medios y medidas disponibles la ejecución del acto penalmente prohibido. En Ecuador no existe este tratamiento de la delincuencia organizada como un contexto de otra actividad delictiva tipificada. El único aproximamiento que sobre la delincuencia organizada es como un tipo definido en Art. 369, de titulado homónimamente, que sanciona la acción de concertar la conformación de una estructura criminal, pero sin tomar nunca que esta será usada de plataforma para la consumación de otras actividades delictivas como un factor que influya en estas mismas actividades de manera consistente. A criterio personal, esta posición es deficiente y errónea en la ley ecuatoriana ya que descontextualiza por completo el concepto de delincuencia organizada y su impacto dentro de otros tipos a los que estas se ajustan, en especial el informático, que tras la comprensión de la escala sobre la cual se podía sacar ventaja, fuer ampliamente adoptado por estas organizaciones y se ha vuelto sinónima de estas. El no considerar un agravante o hacer una mención o formulación de estas estructuras, ahora fundamentales y simbióticas con el fenómeno de ciberdelincuencia, es no contextualizar la gravedad, la escala y la coordinación con las que estas pueden ser usadas para atacar un sistema informático de interés para estas organizaciones, que por razones derivadas de su ocupación, rara vez significa la realización de un solo tipo penal, ya que este uso de la informática es una herramienta para la comisión de delitos más severos, afectando así otros bienes jurídicos.

Artículo 249

1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:

a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

(…)

2. Con la misma pena prevista en el apartado anterior serán castigados:

a) Los que fabricaren, importaren, obtuvieren, poseyeren, transportaren, comerciaren o de otro modo facilitaren a terceros dispositivos, instrumentos o datos o programas informáticos, o cualquier otro medio diseñado o adaptado específicamente para la comisión de las estafas previstas en este artículo.

La estafa es una figura que se contemplan en las dos legislaciones a comparar. En la española se codifica en su artículo 248. En la ecuatoriana, es el artículo 186. Y entre estos no hay virtuales diferencias, al menos no substanciales, salvo sobre la atención que prestan los dos cuerpos respecto de la estafa en medios informáticos. La ley en el reino de España eleva las caracterizaciones más particulares del tipo de estafa. Entre estos, una de las adiciones más importante es una caracterización amplia de las modalidades de estafa que se involucren a través de la manipulación de los datos como se describe en el literal a) del numeral primero; o a través de software o hardware como en el literal a) del numeral dos. Este desarrollo es adecuado respecto de la problemática, ya que no solo la tipifica, sino que la describe específicamente respecto de los elementos más fundamentales, y por tanto inmutables, de la informática que son el Software y el hardware. El Ecuador palidece en este aspecto, quedando la única mención medianamente relacionada a la informática, reducida a la mera estafa a través de tarjetas; y quedando disperso lo que se conoce como estafa informática a través de una variedad de delitos del Código Orgánico Integral Penal, que se pueden seguir a través del inter criminis, pero por el simple hecho de no estar adecuado a un tipo o descrito formalmente dentro del más natural que es la estafa, el intento de adecuarlo al resto de figuras se vuelve más complejo, y por lo tanto menos efectivo volviéndose hostil ante la ciudadanía, y dificultando la consecución de la justicia a través de una sentencia.

Artículo. 264

1. El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.

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

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

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

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

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

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

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

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

Artículo 264 bis

1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizará o interrumpiera el funcionamiento de un sistema informático ajeno:

a) realizando alguna de las conductas a que se refiere el artículo anterior;

b) introduciendo o transmitiendo datos; o

c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

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

Artículo 264 ter

Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los dos artículos anteriores; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Los artículos 264, 264 bis y 264 ter hacen un desarrollo continuo y consecutivo de las

condiciones y términos de la actividad de supresión de datos o sistemas informáticos. Contextualizando que buena parte del sistema público y financiero moderno dependen en buena medida de estos sistemas y la información en ellos contenidas para su correcto funcionamiento, es consecuente entender que la inhabilitación de uno alguno de estos dos, o ambos, puede culminar con la suspensión del correcto funcionamiento de todos estos sistemas, y por tanto terminar vulnerando múltiples bienes jurídicos. La escala de afectados es altamente dinámica, pudiendo pasar la afectación de unos pocos a una porción importante de la población. Entonces, entendiendo que la afectación tiene una graduación en función de la escala, los mencionados artículos de la legislación del Reino de España hacen una apreciación sobre sus consecuencias jurídico-penales en igual grado, aunque inversa, empezando desde la variante más grave hasta la menos grave en su descripción en el articulado. El primero, el 264, introduce la conducta, en lo que podríamos denominar su forma estándar, que, entendido su impacto como uno de alcance menor, responde a una pena que abarca desde los seis meses, el límite entre la pena y la contravención; a tres años. Seguido de esto, los numerales agravan la pena en función del aumento en agravio consecuencia del acto, se contextualiza su cometimiento en organización criminal como un agravio al entender que la acción deriva entonces de la intención de aportar en la coordinación, financiamiento o auxilio de otros actos delictivos futuros, presentes o pasados. Se señala también progresiones en condena en caso de que el daño afectara múltiples sistemas informáticos, sistemas críticos para la infraestructura pública o hubiera afectado los sistemas de la Unión Europea, integrándose aquí el componente comunitario derivado de la susodicha unión y el Consejo de Europa; teniendo todas estas penas una sanción más grave, una que abarca desde dos a cinco años; pero teniendo como condición para el agravio de la pena la figura de la extrema gravedad, que se analizara en función del daño.

El artículo 264 bis es un artículo que expone una conducta que comparada con la que introduce el art. 264, es de menor gravedad, esto se expone ya que la conducta es virtualmente la misma determinada en el artículo base, pero sin el requerimiento de que los daños sean graves. La conducta descrita es la de obstaculizar el funcionamiento ajeno; siendo el termino ajeno uno que se refiere a la población en general, puesto que para sistemas de mayor importancia existen términos más específicos; dedicándose el articulado a contextualizar donde se delinean los límites de la gravedad de la conducta al redireccionar la sanción correspondiente a este artículo, al artículo base, en caso de que las acciones se enfrascaran en circunstancias que ahí se describen.

Por último, artículo 264 ter contextualiza los aportes de software para la realización de las actividades antes descritas, sin llegar a ser participe, llevando una sanción menor, una desde los seis meses a los dos años.

En la república ecuatoriana contamos con articulado que abarca está actividad, pero la exploración sobre la naturaleza, condiciones y contexto del delito no existen, al menos no al nivel de la que hace el Código Penal Español. En Ecuador lo abarcado en este artículo se encuentra disperso entre varios tipos penales con sus distintos artículos. Los artículos serían 232, el ataque al sistema informático, 233, la alteración y eliminación de datos públicos, el 234.1, de la alteración de los datos en general y el 234.2 de la valoración de la gravedad de las consecuencias derivados de estas actividades antes detalladas. Al tipificarse por separado, estos delitos no miran como tal una actividad conjunta en evolución según la gravedad, como sí lo hace la ley española; más bien, los escenarios se analizan como conductas aisladas e independientes. Una perspectiva errónea, debido a que esta descripción no comprende como las fronteras entre estos tipos muchas veces se superponen en su cometimiento, con una acción llevando a la otra, y resultando en qué se procese la pena más grave por concurso ideal, quedando los otros delitos como accesorios que rara vez actúan independientemente; razón por la cual al legislación española, consciente de este factor, engloba el comportamiento de atacar un sistema, que es la acción más básica en los delitos informáticos, y a partir de ahí desarrolla una seria líneas descriptivas que permiten delimitar como la sanción se maneja a través de la evolución de la acción en función del uso de ciertas artilugios, programas o información, pero siempre permaneciendo dentro del mismo tipo penal.

El punto a señala no es que no se deba separar los tipos; después de todo estos cuentan con elementos constitutivos diferentes, y hay partes en delitos organizados que intervienen hasta cierto punto. No obstante, es deficiente que estos no hayan sido vinculados en sus respectivos tipos, más allá del agravante por afectar sistemas críticos; tomando en cuenta que este tipo de actividad delictiva se coordinan en cadena lógica con elementos de todos estos tipos para el cometimiento de alguna infracción final, que al final subsumirá a las otras por gravedad en concurso ideal. La gran tarea en estos aspectos de la legislación es delimitar hasta donde cada una de las actividades descritas en el delito, pasan a formar parte de otra más grave o se engloban en la totalidad de un ataque informático.

Artículo 270

1. Será castigado con la pena de prisión de seis meses a cuatro años y multa de doce a veinticuatro meses el que, con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero, reproduzca, plagie, distribuya, comunique públicamente o de cualquier otro modo explote económicamente, en todo o en parte, una obra o prestación literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

2. La misma pena se impondrá a quien, en la prestación de servicios de la sociedad de la información, con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios.

3. En estos casos, el juez o tribunal ordenará la retirada de las obras o prestaciones objeto de la infracción. Cuando a través de un portal de acceso a internet o servicio de la sociedad de la información, se difundan exclusiva o preponderantemente los contenidos objeto de la propiedad intelectual a que se refieren los apartados anteriores, se ordenará la interrupción de la prestación de este, y el juez podrá acordar cualquier medida cautelar que tenga por objeto la protección de los derechos de propiedad intelectual.

(…)

4. En los supuestos a que se refiere el apartado 1, la distribución o comercialización ambulante o meramente ocasional se castigará con una pena de prisión de seis meses a dos años.

(…)

5. Serán castigados con las penas previstas en los apartados anteriores, en sus respectivos casos, quienes:

a) Exporten o almacenen intencionadamente ejemplares de las obras, producciones o ejecuciones a que se refieren los dos primeros apartados de este artículo, incluyendo copias digitales de las mismas, sin la referida autorización, cuando estuvieran destinadas a ser reproducidas, distribuidas o comunicadas públicamente.

(…)

c) Favorezcan o faciliten la realización de las conductas a que se refieren los apartados 1 y 2 de este artículo eliminando o modificando, sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, las medidas tecnológicas eficaces incorporadas por éstos con la finalidad de impedir o restringir su realización.

d) Con ánimo de obtener un beneficio económico directo o indirecto, con la finalidad de facilitar a terceros el acceso a un ejemplar de una obra literaria, artística o científica, o a su transformación, interpretación o ejecución artística, fijada en cualquier tipo de soporte o comunicado a través de cualquier medio, y sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios, eluda o facilite la elusión de las medidas tecnológicas eficaces dispuestas para evitarlo.

Será castigado también con una pena de prisión de seis meses a tres años quien fabrique, importe, ponga en circulación o posea con una finalidad comercial cualquier medio principalmente concebido, producido, adaptado o realizado para facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador o cualquiera de las otras obras, interpretaciones o ejecuciones en los términos previstos en los dos primeros apartados de este artículo.

Como se indicó con anterioridad. Un componente fundamental dentro del derecho informático es la regulación del contenido que se mueve por los sistemas y consecuentemente, por las redes. Este artículo de la legislación española enlista las actividades punibles penal y pecuniariamente dentro del estado español, respetando así el Convenio de Budapest en su Artículo 10. El desarrollo descriptivo de este articulo regula en líneas generales las actividades delictivas hacia el derecho de autor y la propiedad intelectual. Imponiendo una pena privativa de libertad que abarca desde los seis meses hasta los cuatro años, este margen tan amplio en la pena probablemente derive del rango de magnitud que puede derivar de estas actividades, que, según las circunstancias,

pueden significar afectaciones menores, como la distribución entre amigos de una película sin licencia, y mayores, como la distribución organizada y diseñada de contenido sujeto de derechos de autor a una escala equiparable con el streaming. Este articulo además les da capacidad a los jueces para desarmar, desarticular y dar de baja los lugares, sean estos físicos u online, que den acceso al contenido sancionado en este artículo, y la capacidad de ordenar su retiro de plataformas online. En Ecuador las regulaciones respecto del derecho de propiedad intelectual corren respecto de lo que está escrito en el Código Orgánico de la Economía Social de los Conocimientos, y las sanciones están establecidas en el Código Orgánico Integral Penal en artículos 208A y 208B, igual que en la ley española en estos artículos se tipifican múltiples actividades.

Los artículos de la legislación ecuatoriana hacen primero una categorización entre actos lesivos a la propiedad intelectual, que tienen una relación aparente con patentes; y actos lesivos contra la propiedad intelectual, derecho resultante de la propiedad intelectual que se ejerce respecto de lo que autor puede hacer con su obre; en los cuales se describe de manera amplia las actividades delictivas que son lesivas para cada uno, de manera separada, y en detalle. Esta separación es más simple para entender, y hace una gran distinción sobre qué bien es aquel que se está lesionando exactamente. Ambos artículos, tanto el 208A en Ecuador, como el 270 de España, abarcan los actos que van en contra del derecho de autor, es decir, sobre este derecho exclusivo que tiene el autor para determinar los medios sobre el cómo ha de explotarse su obra. En el caso de la legislación hispánica, el articulado si bien tiene aplicaciones sobre otras formas de distribución predecesoras al dominio de la web, tiene un fuerte enfoque sobre el uso de las plataformas web o informáticas para la distribución masiva de las mismas. La ecuatoriana por su parte es mucho más ambigua respecto del aspecto informático. Se trata las modalidades sobre las cuales se lesiona el derecho de autor, de manera específica, es decir a través de que mecanismo material se configuro y como se obtuvo; y no tanto respecto de a través de mecanismo se distribuye. Por lo cual, la ley ecuatoriana deja ambigua la cuestión de la distribución, copias, alteraciones o replicaciones de material sujeto de propiedad intelectual en las redes. La actividad puede acoplarse al tipo, sin embargo, no queda claro a través de su exposición escrita al faltar el uso del vocablo informático y sus derivados para aclarar ciertas modalidades.

4.5.2 Legislación chilena: Ley 21459

La legislación penal chilena contaba anteriormente con una única ley que tipifica los delitos informáticos, la Ley 19223, que constaba de tan solo 4 artículos, no obstante, al estar el estado

chileno integrado al Convenio de Budapest, en junio de 2022 se publicó la Ley 21459, que derogaba la ley anterior, e incorporaba tipos informáticos acorde a los términos del Convenio. Esta ley tiene como intención el tratar estrictamente los que serán considerados como delitos informáticos dentro de la República de Chile y como tal, es una excelente contribución al estudio comparativo al encontrar un cuerpo jurídico que define en líneas estrictas sobre cuales son delitos informáticos de una manera sencilla, y en línea con el convenio de Budapest, su explicación simple, permitirá que a través del contraste se pueda apreciar aportaciones significativas.

> **Artículo 1°. -** Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Como se expuso, y se expondrá por última vez pues se sobre entenderá que a los siguientes delitos aplica igual condición; los términos de le legislación chilena son simples, pero también muy generales. El artículo uno de esta ley define el ataque a la integridad de un sistema informático en dos verbos: obstaculizar o impedir, verbos relacionados a la alteración del funcionamiento normal, o usual de un sistema. Lo que prosigue a estos verbos es meramente una descripción del objeto, el sistema, y de los medios, exponiéndolos en gravedad, y muy sumariamente. La pena expuesta es descrita como presidio menor de grado medio, que dentro del régimen penal chileno equivale a una pena de privativa de la libertad de 7 meses (541 días) a tres años. En la República chilena, por tanto, el simple accionar que termine como resultado en poner fuera, causar malfuncionamiento o baja de un sistema, cualquiera fuese la intencionalidad por la cual se llegó a ella, responde sobre este artículo, sin acciones que se puedan considerar accesorias o de características similares descritos plenamente. En Ecuador la exposición sobre este delito es muy diferente, primero porque el Art. 232, de título homónimo, hace una exposición de acto tipificado que por su formulación requiere del dolo en su actuar para acoplarse al tipo. Esto cuando expone que la acción se ha de realizar "con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático" (Código Orgánico Integral Penal, 2014, Art. 232, p. 77) un elemento que la ley chilena no tipifica y, por tanto, con arreglo de los principios del derecho penal, no existe como requisito. Toda actividad que resulte en estos hechos en territorio chileno se sancionara con la pena antes descrita, de resultar las condiciones requeridas en el artículo. En Ecuador, se requiere que además del resultado, se pruebe la existencia del dolo expresado tácitamente en el extracto

antes citado, es decir, de no comprobarse la existencia de este elemento de dolo, de esa necesidad de causar un parón grave, deliberado e ilegitimo, no se configura totalmente el tipo penal, permitiendo quizá una ventana para lo que se conoce como hacking ético, o de sombrero blanco, o una desestimación del carácter delictivo de la acción ante acto culposo, entendiendo que a este caso lo atienden los reclamos de la vía civil sobre los daños causados. La ley ecuatoriana también desarrolla sobre la misma pena y modalidad, actividades que serían accesorias al delito de ataque la integridad de sistemas informáticos, como lo es el desarrollo de software con el preciso propósito de acaecer las condiciones expone en su primer inciso, sumada a la incorporación de un agravante constitutivo destinado a la protección de la información y los sistemas que el estado usa para dar sus servicios a la ciudadanía, entendiendo que su afectación resultaría en una eventual vulneración de múltiples derechos y garantías constitucionales, estableciendo una pena más dura en el rango de cinco a siete años.

> **Artículo 2°. -** Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.
>
> Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimos a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.
>
> En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

La ley chilena expone en su segundo articulado el acceso ilícito. La condición para la conformación como tal del delito se expone en que el acceso debe hacer sin autorización, o excediendo la autorización, es decir excediendo aquellos limites que se la han impuesto, yendo contra norma o acuerdo, exponiendo así un carácter antijuridico. Sumado a esto se expone que este accionar debe hacerse superando las barreras técnicas que se hayan formulado específicamente para el caso. Este apartado infunde un carácter técnico al delito, ya que las barreras de seguridad son sistemas de cerrojo o protección cuya configuración esta mayormente provista para evitar que se pueda acceder por medios o conocimientos normales; pudiendo categorizarse como un delito de

cuello blanco.

La condición de superar barreras de seguridad existe para dejar fuera de las contemplaciones de este articulo a escenarios como el acceso a un dispositivo que por descuido del usuario deje a simple vista o acceso la información, de tal modo que no basta con el simple hecho de haber accedido superando la autorización del usuario; se necesita también que haya habido un acto de superar las precauciones tomadas con el fin de demostrar que la acción fue en contra de la voluntad de mantenerla fuera del alcance de otros. Por poner un ejemplo, la persona que encuentra un teléfono sin clave, y accede a él para saber de quién es y retornarlo; está teniendo acceso a la información del usuario, y sin su autorización. Sin embargo, no ha superado ningún sistema de seguridad o informático en el proceso, la información carecía de cualquier seguro, y ante esto, cualquier persona por la mera casualidad de interactuar con el equipo podía acceder a esa información sin así quererlo. Entonces concluimos que no basta el acceso no autorizado, se requiere además ir en contra del deseo del acceso a la información expresa en las precauciones y barreras que se superen. En una analogía más terrenal y fuera de los dominios informáticos, el acto de abrir correspondencia ajena es un acto delictivo, no obstante, si la carta se viera fuera de su sobre y cayera en la calle, a plena vista del mundo, se accediendo a su contenido sin el consentimiento del titular de la carta, pero en ningún momento se vulnero sus protecciones y el deseó de protegerlo o evitar su lectura por parte del titular no se puede asumir, si es que alguien llegara a leerla, no existiendo por tanto una acción de vulneración y dejando a quien la lea fuera de cualquier responsabilidad penal. Este accionar se sanciona con una pena que se enmarca en el rango de 61 días a 301 días.

La legislación chilena desarrolla además de lo antes mencionado, un agravante constitutivo en casos de que el acceso se haya dado con el propósito de capturar datos que se encontraban en el sistema. Igual pena se le da a quien divulgue la información capturada en dos escenarios. El primero, que la divulgue sin haberla conseguido el sujeto activo, la cual responde a la misma pena que la captura de los datos, una de responderá de 7 meses a 2 años. El segundo escenario tiene efecto cuando la persona que divulga los datos también es aquella que accedió ilegalmente y capturo los mismos se sancionara desde 819 días a 1,095 días de pena privativa de la libertad.

La ley ecuatoriana contempla esta actividad bajo los artículos 229, 230 y 234. El 234 engloba el acto de acceder a un sistema, diferenciándose de la legislación penal por el hecho de que además de los términos que requiere la ley chilena, se debe permanecer dentro del sistema

violando voluntad en contra del titular del sistema. Además de esto, la pena es superior y no se trata sobre la captura de la información. Sobre esto último intercede el 230 que, además de ser más severa en pena que la legislación penal chilena, toma en cuenta muchos más aspectos de la interceptación de los datos, estimando incluso la mera posesión de los datos, el desarrollo del software medio. Respecto de la divulgación, el artículo 229, que sanciona de uno a tres años, cuando se revele la información que se encontrase almacenada en algún tipo de base de datos o ficheros, siendo agravante constitutivo el ser funcionario público, ya que se entiende que actúa en violación de la confianza que de su rol deriva, dictándose sanción de tres a cinco años de pena privativa.

> **Artículo 3°. -** Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.
>
> El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Respecto del artículo tres, en términos generales, la legislación chilena y la ecuatoriana no varían significativamente en términos de los elementos constitutivos del delito, viéndolo ambas incluso como un tipo con una pena que se podría considerar indulgente. No obstante la legislación chilena diferencia la intercepción indebida y la no autorizada, haciendo una suerte de diferenciación en el nivel de consciencia, mientras que el indebido es el acto de actuar en contra del comportamiento que se entiende es debido, y por tanto podría entenderse como una identificación alterna del error, ya que indebidamente se accedió al sistema; el acceso sin autorización es un acto de actuar sin ninguna virtud o condición legal que lo permita, y por tanto, contra derecho, porque es el quebrantamiento de la condición habilitante, la autorización, y por tanto es más grave, sancionándose en consecuencia con un grado mayor de presidio.

Por supuesto, la ley ecuatoriana es más extensa en la expresión de lo que considera este delito, exponiendo actos que incurren en la violación de este bien, pero en diferentes modalidades; mientras que la chilena por su parte se concierne únicamente con describir el comportamiento antijuridico y la afectación del bien, sin interesarse en las cuestiones relacionadas a los modos de

realización.

> **Artículo 4°. -** Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Si bien son homónimos, el artículo 4 de ley chilena, y el artículo 232 del Código Orgánico Integral Penal, mantienen la línea de sus dos cuerpos legales.

El articulado chileno establece únicamente la conducta general lesiva, es decir el acto concreto en verbo que lesiona el bien, sin merecerse en detallar las circunstancias. El artículo ecuatoriano, haciendo una descripción detallada de las múltiples circunstancias del hecho. Para exponer esta dinámica haremos una simple comparación.

El articulo 4 usa tres verbos para describir la afectación de los datos, por otro lado, el 232, usa diez, y mientras que el articulado chileno expone como bien afectado los datos informáticos, la ley ecuatoriana toma sistemas informáticos, sistemas TIC, dispositivos electrónicos e infraestructura tecnológica, lo que plantea la pregunta ¿si el dispositivo afectado no entra dentro de estas descripciones?

Este punto es importante, porque mientras que la legislación ecuatoriana trata de detallar tantos medios o verbos como sea posible en la intención de extender la protección tanto como sea posible literalmente. Irónicamente, el resultado es contraproducente pues el uso tan especifico de los verbos, recordando siempre que en el derecho penal la literalidad es inexpugnable; termina por crear un tipo muy estricto que con las innovaciones y cambios de denominación propios de la tecnología quedan obsoletos e ineficientes.

La ley chilena por otro lado ofrece una protección más eficiente, ya no se refiere de los medios informáticos o electrónicos, al fin al cabo estos son únicamente medios de interacción o almacenamiento del elemento fundamental de este delito: los datos informáticos. A través de establecer que debe haber alteración, daño o supresión hacia los datos, se cubre básicamente cualquier modalidad de presente, futura o pasada, y todos los mecanismos que puedan surgir en el camino siempre que contengan datos, ya que como el nombre sugiere, el objetivo de la actividad que sanciona este artículo, no son en si la infraestructura los contiene, cualquiera esta fuera; sino los datos en sí, y como tal siempre tendrán una afectación sobre estos, requiriéndose únicamente como requisito extra que la alteración se indebida y cause daño grave.

Este artículo es una clara representación de por qué no se necesita tipificar en la ley cada

modalidad especifica de los delitos que se quiera sancionar, puesto que la descripción excesiva vuelve ineficiente al artículo ante los delitos que tienden al cambio y la adaptación. Lo que funciona es encontrar el componente fundamental común que atacan estas modalidades, de tal modo que no importa como estas cambien, seguirán encajando en el tipo.

> **Artículo 5°. -** Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.
>
> Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

En ambas legislaciones se hace una descripción que más allá de palabras específicas, son en esencia el mismo tipo. Tanto el artículo 5 de la ley chilena, el 234.1 de la ecuatoriana, describen una conducta que a través de cambios introducidos, cambiados o suprimidos de datos informáticos se busque inducir una apariencia de validez no existente, un acto doloso y premeditado por su naturaleza debido a que se hace las debidas reservas y cambios para asegurarse de engañar al sujeto pasivo con conocimiento de que el accionar va contra ley expresa; variando esta descripción del enunciado base únicamente respecto de la pena que en la legislación pena pues en la legislación penal chilena se puede establecer dos márgenes de pena para una misma sanción penal, que en el caso de esta conducta se establece en presidio menor en grado medio, es decir de 541 días a tres años; a presidio menor en su grado máximo, de tres a cinco años. En este aspecto el Ecuador mantiene una línea más simplista, que en este caso es una mejora respecto al chileno en su lectura y análisis, estableciendo una pena de margen único que abarca desde los tres a los cinco años de pena privativa de la libertad, tanto como la conducta base como en conductas derivadas, siendo además más severo respecto de la conducta básica ya que el margen mínimo de la pena ecuatoriana es por mucho mayor a los 541 días que supondrían el margen mínimo de la chilena.

Como se explicó, ambos códigos cuentan con una conducta base idéntica en elementos constitutivos y diferenciada únicamente en la sanción. Sin embargo, ambos cuerpos legales extienden sus enunciados a un segundo inciso, en el caso de Chile, y numeral, en el caso de Ecuador, cada uno apreciando algo que el otro cuerpo de ley no contempla, una sería de conductas

derivadas que responden al mismo tipo, agravando en la primera, y bajo la misma sanción en la segunda. El segundo inciso del texto chileno contempla el accionar de un servidor público en las conductas descritas en el primer inciso y apreciando el abuso de una posición en el sector publica que ostenta una dignidad de confianza, estima la traición de esta misma y el abuso de las potestades otorgadas por dignidad estatal que el sujeto activo porte, como un agravante que sube los márgenes de sanción sobre los que ha de responder a los de presidio menor en grado máximo, es decir de tres a cinco años, o presidio mayor en su grado mínimo, que abarca desde los cinco a los diez años. Una contemplación como esta no existe dentro del articulo formulado en el Código Orgánico Integral Penal, lo cual es ciertamente llamativo debido a que en otros artículos relacionados a la informática como 229, y 233, esta contemplación existe; no obstante, en el 234.1 no existe como tal, sabiendo que los funcionarios públicos por su cercanía a documentos, datos o bases tienen una ventana de oportunidad única para este tipo de actividades. Así tampoco se contempla en los agravantes del 234.2, lo que al criterio de este trabajo se aprecia como una falla solida del articulado ecuatoriano.

Por su parte, el numeral dos del artículo 234.1 del Código Orgánico Integral Penal expone una conducta consecuente del cometimiento del primer numera, estimando que tiene igual responsabilidad penal, y sanción idéntica, quien con dolo o intención de obtener beneficio personal o de un tercero, use un documento producto de la falsificación original.

Este enunciado parece seguir un inter criminis, estimando que el forjamiento o falsificación de un documento, puede tener un origen en un personal técnico o que tenga acceso al documento, pero tener como destinario de uso, y por lo tanto actor intelectual, a un individuo que lo solicite para su uso personal o de un tercero. Este segundo inciso no se contempla en ningún momento dentro de este cuerpo chileno, ni es el artículo 5, ni en el 9 que habla de los agravantes. Y es preciso mencionar que esta apreciación del Código Orgánico Integral Penal muestra un mejor uso de la descripción para establecer los límites de la responsabilidad penal derivada que el chileno, en el cual una situación como esta, no podría responder al tipo que se establece en norma, debido a que este en su formulación contempla únicamente un individuo “El que indebidamente” (Ley 2149, 2022, art. 5, inciso primero) y hace referencia únicamente a verbos relacionados con el cambio, nunca con el uso.

> **Artículo 6°. -** Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u

otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

Ha de señalarse primero que nada que una tipología independiente como esta no existe en el Código Orgánico Integral Penal, encontrándose disgregada a través de diferentes incisos y numerales correspondientes a cada tipo. La receptación es interesante como un articulado singular, ya que a pesar de estar separada de los artículos que le preceden, aun así, solo responde y toma efecto respecto de ellos, el 2º, 3º y 5º. Que para efectos prácticos tiene el mismo efecto real que si estuviera incluido un numeral, inciso o cualquier tipo de apéndice dentro de cada uno de ellos, por lo cual las diferencias en efecto con la legislación ecuatoriana son nulas, salvo el mencionar que estas existen en diferentes clasificaciones, y que la legislación chilena presenta una ventaja desde un punto de la pedagogía y la legibilidad, ya que en lugar de tenerse presente cada artículo con cada una de estas condiciones idénticas establecidas dentro de ellas, es mucho más practico comprender la acción en general, y entender sobre qué casos aplican según establece su propia indicación.

Artículo 7°. - Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.

El delito de fraude informático tiene una particularidad en comparación con el resto de los delitos. Esta es el hecho de que este es delito estrictamente económico, es decir el daño no está en la afectación de los datos, está en la afectación del patrimonio de un sujeto pasivo con el uso de infraestructura, programas o datos informáticos. Es decir, existe una clara diferenciación sobre qué cosa cae la afectación, y la pena tiene una sanción más grave en conforme con que aumenta la afectación económica. Este delito no existe como tal en el Ecuador, existen los delitos informáticos que se han expresado hasta este punto, que sancionan sobre los daños a los datos y las infraestructuras donde estos se almacenan; y existe el delito de estafa, que subsume al fraude en sus elementos constitutivos y definiendo en términos generales que el acto de engañar a alguien para afectar su patrimonio en favor del sujeto activo a través del uso del engaño es estafa. Realmente, el delito de estafa básico, tal y como esta descrito en el primer inciso de artículo 186 es practico para poder perseguir el fraude informático porque su intención describir el accionar sancionado en términos tan generales, cubre bajo su sombra de alguna manera este mismo delito. Sin embargo, cabe mencionar que la separación o instauración de una figura especial para el fraude informático presenta un beneficio derivado de haber aislado elementos específicos de la informática y mantener siempre como bien afectado el patrimonio económico, que es la celeridad que deriva de tener un proceso donde el carácter informático no debe comprobarse, pues estaría expreso en los términos el involucramiento de estos dispositivos, programas, etc. Y se resumiría meramente a probarse sobre los hechos sucedidos en estos y si las acciones fueran lesivas.

Artículo 8º.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados

principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.

El principal aporte a la discusión del artículo 8 radica en como establecer al uso dispositivos, programas, y contraseñas no solo dentro del contexto de un delito que ha de suceder con resultado o tentativa en la cual se haya visto involucrado un programa, para acoplarlo como participe en la misma actividad y darle una pena como hace el Código Orgánico Integral Penal. Sino también debe configurárselo de manera independiente al simple diseño, uso, importación, distribución o divulgación de mecanismos y herramientas que sirvan como mecanismos para vulnerar la ley, aun cuando estos no se hayan llevado a cabo, ya que el simple hecho de adquirir, diseñar, importar o véase cualquier interacción con propósito de facilitar mecanismos para la comisión de un delito, debería estimarse como uno.

Cabe señalar que el aporte no es en sí como en el artículo anterior el hecho de tener un artículo que tipifique por separado una condición que afecta a un cierto grupo de delitos en lugar de estar estos expresados en cada uno. El aporte es el tener la situación de facilitar software y hardware con propósito malicioso fuera del contexto de la actividad penal resultante, con una pena; y apartar tener este mismo comportamiento en cada uno de los delitos, contextualizado en su gravedad debido al delito resultante que requirieron de los mecanismos ofrecidos. Es decir, una pena por el proveer de una sistema o mecanismo con propósito malicioso, y otras más graves, adscritas a cada tipo penal especifico que el mecanismo o software ayudo a suceder, en función de los gravosos que estos fueran.

4.5.3 Legislación argentina: Código Penal de la Nación

La legislación argentina es la más particular de las exploradas a causa de la naturaleza federal del estado argentino, que deriva en legislaciones procesales propias de cada entidad federal, en este caso las provincias, pero regidos bajo una ley penal nacional que simplifica el exponer su aproximación.

Dentro del Código Penal de la Nación Argentina, no existe como tal un título, capitulo o apartado dedicado a los delitos informáticos como tal. Sin embargo, se puede identificar como tal todos los delitos que se incorporaron o se reformaron por la modificación que realizo la Ley 26.388 en el 2008 al ya mencionado Código y otros articulados contemplados en el mismo cuerpo.

ARTICULO 128 — Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por

cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.

Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

La legislación argentina hace una apreciación de mayor amplitud a la que el Convenio se apega, tomando el rango total que comprende la minoría de edad, donde el Convenio de Budapest solo se pronuncia respecto de los aspectos relacionados estrictamente a la pornografía infantil.

El enfoque del tipo vigente dentro del Código Penal de la Nación Argentina aprecia el derecho a la integridad y la dignidad de los menores en mayor detalle, al extender los elementos del tipo en la medida del rango de lo que legalmente se consideran menores de edad en su legislación, que es la edad de los 18 años. El artículo describe como penalmente punibles las conductas que están conducidas a facilitar la producción de material pornográfico, el cual se trabaja detalladamente respecto de que se califica como tal, estableciendo que es la representación en contexto sexual de menores, ya sea en actos, representación de sus partes y estableciendo una pena de tres a seis al responsable del origen del material.

Si bien el artículo no hace mención en ningún momento respecto del uso de los medios informáticos, es más en ningún momento se menciona respecto de los tipos de almacenamiento o medios de distribución. La ley argentina tipifica los actos sin importarle estas cuestiones, sancionando así sobre cuestiones como la mera posesión con conocimiento de la edad del menor,

posesión con intenciones de comercialización, y facilitación y suministro del material. Estimados del menos grave al más grave. En ecuador el Código Orgánico Integral Penal adscribe la pornografía infantil en el 103, en términos más acordes con la visión moderna del acto delictivo, conteniendo en el plenamente medios electrónicos e informático, haciéndose una descripción sobre los soportes de la acción y una contemplación impasible sobre el origen del material, desestimando por completo la condición de conocimiento de la edad del menor que la legislación argentina si tiene; y sancionando de trece a quince años sobre quien, de origen al material, una mucho más grave que la sancionada en Argentina.

Respecto de la responsabilidad penal de los poseedores, distribuidores y responsables de medios de acceso al material que se enumeran en el artículo, la ley ecuatoriana los contempla en el 103 del Código Orgánico Integral Penal, donde todas estas distinciones descritas anteriormente son insignificantes, puesto que ante la justicia ecuatoriana todas sufren igual pena, que es la más grande diferencia entre estas dos legislaciones puesto que donde la más grave de las condenas argentinas sobre estos comportamientos, la de origen, recibía en el máximo de la pena permitida, seis años; en la ecuatoriana los roles derivados reciben una que abarca desde los diez hasta los trece años. Este aumento en las penas puede considerarse como un factor disuasorio ante el consumidor de este tipo de material, debido a la carencia de consideraciones que hace la ley entre persona que distribuye y la que meramente posee, siendo la pena un riesgo muy superior al que las personas ordinarias están dispuestas a aceptar. No obstante, también se podría argumentar que el nivel de riesgo fuerza a quienes cometen este tipo de delitos a hacer más astutos, en concordancia con punto de vista doctrinales del por qué el simple incremento o establecimiento de penas desproporcionadas no es una solución efectiva contra la criminalidad.

> **ARTICULO 131. -** Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

El artículo 131 tipifica la conducta que a nivel global ha tomado el nombre de Grooming, que es la conducta de acercarse por medios informáticos a menores, simular ser otra persona, o tener otra edad, con el fin de seducirlos a concretar acciones sexuales, sean estas en acto o contendió digital. Este comportamiento se entiende como uno de los derivados del fishing, y es especialmente peligroso debido a que se aprovechad el anonimato de las redes y la inocencia de los menores de

edad que carecen de la madures o consciencia para entender estas acciones, explotando de este modo su inmadurez. El Ecuador también tipifica en el Código Orgánico Integral Penal, artículo 173, esta conducta. A diferencia con lo establecido en Argentina, en este tipo se establecen esencialmente dos formas de configurar esta conducta. Una primera menos grave, que implica el contacto con el menor, la proposición de concertar encuentro, y la realización de preparativos materiales que encaminen a una finalidad sexual, lo cual señala la primera diferencia entre este enunciado y el argentino.

El enunciado argentino establece que el simple contacto con propósito de cometer delito contra la integridad sexual es merecedor de pena privativa de libertad, esto quiere decir que no se requiere que exista una concertación de encuentro entre las partes, pudiendo las acciones realizadas únicamente en el ciberespacio ser sujetos de la pena establecida, y que el acto debe tener una intención de cometer delito, es decir antijuridicidad. El enunciado ecuatoriano, por otro lado, expone dos condicionales para que exista responsabilidad penal. El primero es la concertación de un encuentro, lo cual quiere decir que los actos relevantes para la ley son aquellos que toman lugar en plano material, y segundo, que la propuesta venga siempre acompañada de actos materiales encaminada a un acto sexual. Esta última es una condición a la vez que actúa como suerte de prevención, ya que, sin esta, el artículo podría entenderse como una prohibición total de contacto entre individuos con mayoría y minoría de edad. Esto no es así, la concertación entre los individuos es únicamente relevante penalmente si en este encuentro tuvieron lugar acciones que buscaran encaminar la situación hacia el acto sexual; sin este elemento, el delito no existe, y la concertación queda plenamente en legitimada. Esta condición ultima se diferencia con los enunciados argentinos al liberar el delito de la premeditación sobre el dolo. Mientras la ley argentina exige que el contacto busque la comisión de actos en contra de integridad sexual, el articulado ecuatoriano entiende que la conducta puede no es intrínsecamente dolosa, aunque esto no la libere de ser considerada nociva para la sociedad y por tanto merecedora de pena.

Además, para estas apreciaciones ya existen los propios agravantes constitutivos, referidos al uso de la coerción y amenaza, en el segundo inciso, la tentativa, y las propias circunstancias agravantes que se establecen en el Código Orgánico Integral Penal en sus artículos 47 y 48, más específicamente, el numeral tercero del artículo 47 que dice “cometer una infracción como medio para la comisión de otra”, más los que se sumen por su estatus de menor.

La última relación a señalar entre estos dos artículos es aquella respecto del engaño, que la

legislación argentina no contempla en su artículo, ni siquiera como agravante. En ecuador, se establece que la suplantación o la identificación falsa son agravantes constitutivos recibiendo una pena más alta de 3 a 5 años, superior a la común de 1 a 3 años. Este aporte en la legislación ecuatoriana es indicativo de una contemplación más analítica sobre el comportamiento de este delito en sociedad en el momento de formular el tipo.

> **ARTICULO 153. -** Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
>
> En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
>
> La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
>
> Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena.

En Argentina, los delitos, que dentro de la legislación ecuatoriana son 229 y 230 respectivamente, de Revelación legal de base de datos e Intercepción ilegal de base de datos se encuentran recogidos parcialmente en el artículo 153. Este mismo, no es en sí mismo un artículo que se haya formulado con el propósito de plantear sanciones para ciberdelitos, siendo inicialmente un artículo referente a las comunicaciones en general, al que tras reformas posteriores se le agregaron conductas informáticas en consecuencia de su relación con la comunicación. Como tal se establece en esta norma que existe responsabilidad penal sobre la interceptación indebida de datos, que en este articulo no se describen como tal, sino que se ven englobados dentro de términos más generales como telecomunicaciones o comunicaciones electrónicas, que pueden por naturaleza del medio moderno son en datos indiscutiblemente. Este delito es bastante más ambiguo que los expuestos por anteriores legislaciones, y no posee la característica de ser ambiguo como una

intención de cubrir cualquier cambio en el futuro, como lo hace la legislación chilena, ya que el uso de los términos es la respectiva de usos antiguos del lenguaje técnico, y por la forma en que se define, sin establecer una clara relación con tecnologías de la información, datos, bases de datos o ningún tipo de terminología moderna que esclarezca su relación, siendo de esta manera una legislación que pierde su función como un recurso presente en la mente del ciudadano para defenderse, al estar los términos tan anticuados como para que este pueda hacer una asimilación de que el mismo puede abarcar ciberdelitos, o al menos no con facilidad. Como resultado, podemos observar que existe un flaqueo en el uso de las palabras técnicas adecuadas en el tipo frente a la legislación ecuatoriana, que gana terreno en este apartad y desempeña un mejor rol en legibilidad y comprensión a nivel de norma, al expresar explícitamente no solo las palabras técnicas adecuadas, como pueden ser sistemas informáticas, contenido digital, u otros; sino teniendo como auxilio para el efecto una definición clara de estos términos de origen técnico o ambiguos al ojo de quien no lo conociese, en su artículo 234.4. Se puede ver así una apreciación floja sobre el delito informático, y este es un delito informático, que se concluye de solo ver la sanción correspondiente que dentro de la legislación ecuatoriana entraría en el régimen de contravenciones, ni siquiera llegando a delito.

Respecto del 229, la norma en argentina en este artículo expone como un agravante constitutivo la cuestión de divulgar la información conseguida en los términos del inciso anterior. La ley ecuatoriana, más severa en su sancionar de estos delitos, separa la divulgación de esta información en un tipo propio, sobre la cual impone una pena de tres a cinco datos, esta pena no requiere la violación o el acceso al sistema, ya que la información puede ser recibida por un segundo y ser divulgada.

> **ARTICULO 153 BIS. -** Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
>
> La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

El 153 Bis, como se puede inferir por su nombre, fue una adhesión realizada en reforma,

una que buscaba precisamente incorporar una tipología que definiera adecuadamente una conducta lesiva respecto la integridad de un sistema informático. No obstante, y aquí se señala la gran diferencia entre la legislaciones a comparar, este artículo se refiere únicamente de los sistemas del estado o de proveedores de servicios financieros; una apreciación que se lee algo tibia, pues mantiene una pena sobre un acto delictivo que es vigente y requiere un tipificación que es el ataque a equipos, sistemas e infraestructura informática, pero dándole exclusividad a los organismos estatales y financieros, dejando a los equipos de particulares y naturales que no calificaran en estas categorías fuera de la protección de este delito, quedando estos bajo los términos del artículo 183, estimando que los sistemas de las personas antes descritas, jurídicas o naturales, tienen una protección bajo los términos de la propiedad, y no de los datos en sí mismos. La ley ecuatoriana discrepa entonces con la expresión de la ley argentina, ya que los delitos informáticos incorporados dentro del código, que no estén relacionados con delitos sexuales en algún punto, tienen como bien afectado los datos; mientras que la posición argentina, hace una distinción en función de sistemas de organizaciones relevantes para la realidad de ese país, encontrándose la relevancia en los datos particulares que estos manejan, es decir, el presente articulo tiene por bien lesionado los datos; a la vez que estos mismos sistemas en personas naturales y jurídicas que no califiquen en los términos de este delito, son protegidos sobre los términos del 183, que si bien los tipifica y los protege en virtud de tal acción, lo hace con la apreciación de que el bien a proteger es la propiedad, que en este caso sería el sistema, del titular, y no los datos; un punto de vista que se podría someter a debate, pero es muy particular por la apreciación distintiva entre estas dos categorías de sistemas.

> **ARTICULO 157 bis. -**Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
>
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
>
> 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
>
> 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
>
> Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Este es un delito particular para someter a la comparación, ya que, a diferencia de cualquier artículo anterior, este es uno que no elabora sobre un solo acto delictivo, tipificando lo que en la ley ecuatoriana serían tres actos delictivos. El numeral 1, define irrupción forzosa en sistema informático; el numeral 2, la revelación del contenido de bases de datos; y finalmente, el numeral 3, la adhesión/alteración de los datos de un documentos o archivo de datos personales.

Como se evidencia por la disposición de tres actividades delictivas, todas descritas sumariamente, y la estructura que se usó para hacerlo. Este artículo es una exposición de conductas menores cuyo daño es estimado mínimo, pero aun merecedores es una sanción. Casi se podría considerar como un apéndice de actividades delictivas que se contemplan en el código, pero reducidas en pormenorizadas en función de la levedad de sus efectos y por no conjugarse con los resultados materiales que derivan de estas acciones.

Estas acciones existen dentro del código penal ecuatoriana, aunque esta especie de pseudo separación en función de la gravedad, no existe en la legislación. El único factor en la legislación ecuatoriana que puede reducir la pena de la establecida en norma es la presencia de dos atenuantes. Aunque en este caso no hablaríamos atenuantes como tal, pues son delitos independientes pero cuyos elementos están calcados de los términos que establecen los artículos 153 y 153 BIS.

El hecho de tener dos artículos con contenido tan similar, sin elementos que los delimiten o diferencien expresamente establecidos, sumados a que son consecutivos como tales dentro del código, hace que este artículo sea en cierto modo, un menoscabo para el entendimiento de los anteriores mencionados. Por estas mismas razones, se considera a criterio de este trabajo que no existe un aporte que este articulo pueda resaltar a la legislación ecuatoriana, mientras que la situación inversa podría ser beneficiosa para el Código Penal de la Nación.

> **ARTICULO 183. -** Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado.
>
> En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 184. - La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

El artículo 183 y 184 actúan en conjunto, por lo que se los analizara en consecuencia. El artículo 183 es un enunciado que desarrolla sobre los daños respecto de los bienes muebles e inmuebles, y teniendo en cuenta que la relación por defecto sobre estos es la posición de dominio, es uno que trata principalmente sobre los bienes de un individuo. Como se mencionó anteriormente, el Código Penal de la Nación hace una valoración de los sistemas informáticos como un bien inmaterial, inmueble, por tanto, de un individuo. Fue por esta razón que el legislador del Congreso de la Nación, considero al artículo 183, que tipificaba respecto de los daños a la propiedad, como el lugar indicado donde agregar el inciso dos, a través de ley reformatoria, misma que también reformo el artículo 184, que incorpora una serie de agravantes del daño a la propiedad.

La perspectiva respecto del ataque a los sistemas informáticos es precaria, ya que no solo la legislación argentina no entiende el objetivo de la acción que norma, sino que, sumado a esto, le dota de una pena que solo se podría considerar como indulgente y permisiva, palideciendo en contraste con el 232, que no solo es más severo en conducta, sino que entiende el propósito del acto. Lo mismo se puede decir sobre los agravantes que establece el 184, que no tienen su falencia en su formulación o sus elementos, sino en su subestimación de los daños derivados de los efectos de los actos que norman, haciendo especial hincapié al numeral 6, que al igual que el 234.2; es un agravante basado en el daño a infraestructura critica para el funcionamiento de servicios estatales fundamentales, pero que refleja una diferencia brutal en la apreciación de la gravedad reflejada en la pena, ya que la pena argentina , aun en su agravante se limita a los meses para un acto que puede presentar una amenaza hasta a la estructura constitucional del estado, aun cuando el articulo 183 establezca que estos se aplicaran sino fuera un delito más grave que el tipificado, ya que

esencialmente el delito, la actividad penalmente relevante no cambia en su modo, solo cambia en su escala, llegando a ser sometida a un delito que refleja su real impacto cuando el daño resultante sea sumamente dañoso para el estado.

Estos enunciados, cabe mencionar, fueron incorporados en el 2008, al igual que todas las modificaciones que configuraron los delitos informáticos en estos análisis descritos. Esto no se menciona para hacer una historia del tipo, sino para entender que los términos corresponden a una época que se encuentra a 15 años de distancia, precedente a la expansión de los teléfonos móviles, la consolidación definitiva de la globalización informática y a la pandemia del COVID 2020 que forzó una adaptación global de estos protocolos y medios en la población general. Por lo tanto, se encuentran desactualizados en terminología y en concepto, lo cual se evidencia en la tipificación de los ataques a la integridad de un sistema informático, un acto que no tiene un objetivo sobre la propiedad, ya que no busca vulnerar la propiedad del sistema como objetivo, este sería solo un acto medio para el objetivo principal que es la consecución acceso, y manejo del mismo, es decir no se pueden aplicar figuras usuales de la propiedad como la usurpación o daños, ya que no trabaja bajo esa naturaleza. En este sentido, la legislación ecuatoriana sale mejor ubicada respecto a su contraparte, reformada en 2021, configurada por el COVID y el incremento de los delitos informáticos consecuencia de la actividad remota, lo cual ha ayudado a que el Código Orgánico Integral Penal cuente con una legislación, que en cuanto términos y comprensión de los modos operandi, tanto en intención como inter criminis, que, al contraste de la legislación argentina, se evidencia en sus avances legislativos.

4.5.4 Legislación colombiana: Ley 1273 reformatoria del Código Penal Colombiano

La República de Colombia es un país cuya relevancia para el Ecuador es fundamental, como vecino en la frontera norte, y estrecho colaborador de la República en materia de seguridad de Justicia. Por este motivo, es siempre relevante observar los cambios legislativos que se origen ahí, ya que sirven como un campo de observación sobre las experiencias de otros estados cuyas circunstancias y contexto son un espejo curvo de la propia pues no son idénticas, ni siquiera tienen la misma forma, pero en el fondo, se puede definir claramente características que muestran las similaridades entre las dos.

La República de Colombia ha sido desde los ochenta en adelante, una nación que se ha visto resuelta a inmiscuirse en acuerdos y cooperación global. Por lo tanto, no resulta novedoso que Colombia forme parte del Convenio de Ciberdelincuencia de Budapest. Lo que sí resulta

novedoso y digno de señalamiento previo, es el que Colombia pertenece a este convenio desde julio de 2018, cuando se aprobó el convenio en Ley 1928, pero su legislación penal respecto a derecho penal informáticos precede significativamente en tiempo a la adopción antes mencionada, siendo esta expedida en 2009 por Ley 1273 reformatoria del Código Penal Colombiano. Misma que permanecido invariable hasta el día presente debido a estar está en armoniosa concordancia con los términos que establece el Convenio. En este análisis nos remitiremos exclusivamente al fondo de los enunciados, por lo tanto, obviaremos las penas como factor a estudiar, pues la comparación solo se resumiría a mayor o menor.

> **Artículo 269A:** Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

La piedra angular de toda actividad delincuencial en esta área es el primero en describirse en la legislación colombiana, lo cual es un punto muy acertado ya que sigue una proyección de acciones que permite entender como las acciones descritas en adelante serán en cierta forma, evoluciones de este tipo penal. Es más, por el uso real que se le da a la actividad descrita en el tipo, el acceso abusivo a un sistema informático se podría catalogar como un delito medio, es decir, una acción delictiva necesaria para poder conseguir la consecuencia de una más grave, siendo necesario el irrumpir de algún modo en un sistema o base para poder, capturar, secuestrar, alterar, suprimir, o cualquier otro tipo de interacción con los datos o los datos mismos.

La formulación de la conducta en el artículo colombiana contrasta ligeramente con la ecuatoriana. Primeramente, existe una extensión del tipo diferente que se evidencia desde los nombres que se usan para describir las actividades. En Colombia, se describe un acceso abusivo, es decir que supera la confianza, sobre un sistema informático, que es una descripción definida. Por otro lado, en Ecuador se caracteriza la falta de consentimiento, y se extiende la protección a sistemas telemáticos y de comunicaciones, aunque estos ya poco se diferencien de los informáticos. En primera instancia encontramos grandes similitudes en el fondo del texto. La legislación penal colombiana, al igual que hará con todos los artículos de esta ley reformatoria, se acoge a una línea de descripción del acto penalmente relevante ambigua y general en los términos más relevantes, conscientes de que la nomenclatura estricta vuelve a las leyes obsoletas cuando los delitos tienen cambios volátiles, y al igual que en la legislación ecuatoriana resume a describir verbos rectores

que sean fácilmente identificables independientemente del carácter o modo que uso de provecho la acción, como consecuencia los el primer inciso del artículo 234, y el artículo analizado, son esencialmente idénticos en elementos.

La principal diferencia entre estos dos artículos reside en que el código ecuatoriano no solo tipifica el accionar de acceder sin autorización, lo hace con el propósito de explotar el acceso logrado, la alteración un portal web y más importante, ofrecer los sistemas a terceros sin pagar la licencia correspondiente. Esto como se observa no existe en la legislación colombiana, quizá porque se entiende que el enunciado presente en el artículo lo abarca sin mayor necesidad; pero en la legislación ecuatoriana se separó, pues se considera que la intención de explotación es diferente a la mera intromisión, aunque este numeral segundo que se agrega es un poco un despropósito, ya que diferencia una conducta, que se considera consecuente de la primera, pero con un carácter de beneficio propio, sin darle un agravio diferente al establecido para el numeral primero.

> **Artículo 269B:** Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

La relevancia social de las redes e infraestructura informática es innegable. Una parte importante del estado y las entidades financieras depende exclusivamente de que estas estructuras se mantengan funcionando de manera ininterrumpida para poder brindar los servicios sociales. Como consecuencia entonces la república colombiana establece a través de su ley penal que existirá una responsabilidad penal sobre la persona que sin autorización o excediendo la otorgada pause, paralice u obstruya el correcto funcionamiento de los sistemas informáticos de los cuales entidades públicas como privadas dependen, así mismo protege respecto de los datos contenidos en este sistema, por lo cual podríamos considerar que este artículo es la progresión lógica del anterior.

En Ecuador, la legislación se diferencia respecto de su parte colombiana en su detallismo. Mientras se explica que la legislación colombiana se expresa respecto de las acciones en términos generales comunes de todo acto relacionado con la ciber delincuencia, la ecuatoriana en este artículo es obre descriptiva, estableciendo una abundante cantidad de verbos y efectos respecto de la acción relevante penalmente. Este último hecho, sumado al facto de que el articulado ecuatoriano describe a su vez una serie de conductas derivadas. En las anteriores comparaciones se señaló respecto de la tipificación del desarrollo de software y el agravante del ataque de sistemas

informáticos, aunque este segundo inciso tiene una relación similar lo señalado respecto de la legislación chilena con el artículo 269E, que establece el desarrollo de software con propósito delictivo como un delito propio, que lo diferencia de la chilena que lo veía como un agravante de un número de delitos determinado.

> **Artículo 269C:** Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Las diferencias radicales se expresan en las posiciones generales de los cuerpos nuevamente. La legislación colombiana es breve pero eficiente en el uso de los términos. Por su parte, los agregados de la ley ecuatoriana son sumamente específicos y se refieren además de la intercepción, a la manipulación, la naturaleza, y el destino del origen del material digital. La posición ecuatoriana tiene interés superior por establecer una responsabilidad sobre la intercepción informática que vaya más allá del acceso a través de los términos de superar la seguridad, o la capturar material del contenido, procurando tipificar que el comportamiento en general de tener acceso a estos datos, sea incluso por vía observación, si es que este se hizo sin autorización judicial, y en beneficio de un sujeto activo sobre quien sopesaría la sanción, entendiendo que el único requerimiento informático de este delito es que se la información que se obtenga hubiera estado contenida en datos informáticos. De este modo no se requieren necesariamente vulneraciones establecidas en otros artículos en el inter criminis de esta acción, pudiendo proceder respecto de los verbos que determina el artículo.

Para la legislación colombiana, estas cuestiones no son relevantes, determinando en común con la ecuatoriana que la obtención debió hacerse sin orden judicial previa, pero resumiéndose a usar exclusivamente el termino intercepción como verbo rector, considerando irrelevante la existencia o no de un de un beneficio personal, o la necesidad de usar el termino contenido digital por la redundancia, ya que todo contenido digital son datos informáticos, y por tanto describirlos separadamente sino se les caracteriza en diferente gravedad, es irrelevante. Esta posición sobria de tecnicismos es una mejora significativa de la posición ecuatoriana es más eficiente cuando a términos de legibilidad y comprensión viene, aunque flaque al no entender y no exponer el propósito de la acción, ya que este artículo podría limitar gravemente profesiones como el periodismo de investigación sino delimitamos que tipo de intención debe tener esta intercepción,

penalizando así mecanismos externos de transparencia.

> **Artículo 269D:** Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Existe una relevancia especial en la nomenclatura usada en este artículo. Daño informático, una expresión sumamente general, que podría referirse a una afectación a cualquier nivel de un sistema o equipo. Dentro de los sistemas, la unidad común más básica de la informática son los datos, que es su expresión más fundamental se configurarían en código binario, por lo cual una afectación informática es inevitablemente una afectación de estas bases fundamentales en algún modo. Entonces podemos hacer un silogismo simple con las siguientes premisas, el daño informático es una afectación de cualquier parte de un sistema, los sistemas e infraestructuras están construidas medularmente con datos, entonces cualquier daño informático, es en consecuencia una afectación de los datos. Este artículo es compatible en contenido, no en nomenclatura, con el 232 ya esencialmente ambos son enunciados legales que tratan respecto del que altere de una serie de datos, puede ser en contendió, documento o cualquier modo. Por supuesto, a la luz del contraste entre el 232 y este artículo, se puede permanecer la diferencia fundamental entre lo dictado en sus respectivas legislaciones. Es claro que la forma en que se formuló este artículo ha sido premeditada, quizá el proveer una figura penal la cual pudiese responder respecto de afectaciones en el mundo informático, que por las particularidades que este tuviera, no pudieran acoplarse a ningún otro tipo, una especie de segundo filtro para conductas novedosas, ya que ataca los elementos más fundamentales de cualquier tipo de actividad lesiva que se haya dado en el ámbito informático, pues como se mencionó toda acción delictiva en informática es casi siempre lesiva del sistema en algún grado, acoplándose entonces a este artículo. Como punto a señalar del contraste, la legislación ecuatoriana podría beneficiarse de contar con un artículo como este, uno que podríamos llamar como un último recurso en caso de incapacidad de acoplar el comportamiento penalmente relevante a ningún tipo. Y como contrapunto, la presencia de un tipo tan general puede blindar a los actores activos potenciales, al brindarles un tipo al cual se podrán acoger como defensa cuando se les trate de imputar una tipología más grave en pena, pero las reservas de retocarlo que tenga el legislador deberían suplir y solucionar esta cuestión.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Una externalización de un componente agravante en los artículos ecuatorianos. La legislación colombiana, a diferencia de su vecino del sur, ha optado por separar las conductas relacionadas con el involucramiento de programas maliciosos, que en la contraparte es un componente agravante que se incluye en ciertos artículos. Las diferencias entre las dos posiciones radican en que la separación la presente conducta determina que la responsabilidad penal tiene origen desde el momento en que involucren los programas maliciosos. La ecuatoriana por otro lado, al ligar este comportamiento a ciertos tipos específicos, sitúa el origen de la responsabilidad penal en el momento en que el actor provee con los mencionados programas, a un actor secundario que incurrirá en el delito realmente tipificado, ligándole responsabilidad consecuente al actor. Es decir, la conducta no es penalmente responsable sino hasta que se ha involucrado en una acción, haya sido concretada o en tentativa, mientras se encuentre en fase externa, sin valorar que el software tiene un propósito de desarrollo o de adquisición exclusivamente lesiva, que se puede asemejar al hecho de tener un arma sin permisos. Sería entonces oportuno, que la legislación ecuatoriana haga los arreglos necesarios, para además de tener los incisos y numerales que, contextualizado con el resultado del tipo, imponen pena igual que la acción al proveedor de los programas; contar igualmente con un tipo independiente que permita establecer una responsabilidad penal sin la necesidad de que los programas hayan sido usados para el propósito que fueron ideados, siendo el aspecto penalmente relevante el desarrollo/adquisición de programas con orientación a vulnerar sistemas o datos informáticos, con una pena menor

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

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.

> 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.

Una provisión que actúa en contra de actividades del día diario en el mundo de la cibercriminalidad como es el fishing, aunque de una manera indirecta. La piedra fundamental del delito informático es la manipulación y explotación de la carencia de conocimientos técnicos del usuario promedio con el fin de poder conseguir información existiendo dos caminos, la consecución de la fuerza, y la consecución a través del engaño. El segundo camino es esencialmente el terreno fértil para el fishing y derivados, y es por esto mismo que este artículo castiga las suplantaciones de sitios, puesto que este accionar va encaminado a lucrar o aprovecharse de la confianza que da una marca, y que usualmente es usado para conseguir que los usuarios hagan acciones que van en contra de sus intereses o que plano les perjudican económicamente.

Entendido el comportamiento penalmente relevante, corresponde hacer un contraste entre lo dictado en ley ecuatoriana y colombiana. Lo expuesto en el artículo colombiano indica la necesidad de uso un objeto ilícito y la carencia de facultades, programe ya sea páginas, enlaces, comúnmente de redirección, o ventanas emergentes que suelen tener adware. Esta provisión está cubierta por ley ecuatoriana en su artículo 230, numeral segundo, que indica sobre conductas que puedan alterar los nombres de dominio de entidades financieras, o, y aquí se muestran los valores compartidos entre las legislaciones, sitios de confianzas, que puedan inducir el ingreso a una página web diferente a la intencionada de forma engañosa.

Existe un potencial aporte de la legislación colombiana en su último inciso cuando se pronuncia respecto del reclutamiento, entendiendo que estas modalidades delitos han sido uno de los campos fértiles de esquemas financieros fraudulentos que requieren del reclutamiento, cualquier nombre que se pueda darle para el efecto, por su estructura piramidal, una conducta que dentro del Ecuador ha tenido una relevancia importante a razón de incidentes en los últimos años, los cuales no tuvieron un provisión legal concreta que los tratara y por tanto no han encontrado resolución en la justicia.

5. Metodología

La investigación de este Trabajo de investigación requirió de un uso extensivo de varios mecanismos y materiales que fueron valorados como fuentes para poder valorar y razonar las posiciones aquí expresadas.

5.1 Materiales Utilizados

Los materiales bibliográficos de los cuales este trabajo saco provecho académico para su formulación fueron: múltiples obras doctrinarias y jurídicas, códigos, leyes, portales web varios, artículos jurídicos, manuales de interpretación de la ley y diccionarios jurídicos.

Respecto a los materiales no bibliográficos se usaron: computador portátil, cuaderno de hojas a cuadros A4, teléfono celular inteligente, conexión a internet, impresora escáner, hojas de papel bond tamaño A4, fotocopias, etc.

5.2 Métodos y técnicas utilizadas

Con objetivo de configurar adecuadamente este Trabajo de Integración Curricular, se hizo uso en su desarrollo de los siguientes métodos investigativos, que permitieron la producción del conocimiento aquí vertido.

5.3 Métodos empleados

Método científico:

El método científico fue aplicado dentro del trabajo dentro de desarrollo y sustentación del Marcó Teórico, tanto en su parte expositiva, como en su parte comparativa, siendo el mecanismo que, a través de sus procesos, permitió sintetizar las premisas y diagnósticos que sirvieron a la formulación de las conclusiones como producto de lo expuesto.

Método inductivo:

El método inductivo fue usado dentro del Trabajo de Integración Curricular de manera extensiva. Entendiendo que el método inductivo es un estudio que va desde la información particular a la general, se usó extensivamente para poder exponer respecto de las nociones, conceptos y procedimientos que se exponían dentro de la legislación comparada, para luego poder exportarlos al comportamiento general de los códigos que el artículo compusiera, por lo tanto, su uso fue fundamental dentro de la legislación comparada.

Método deductivo:

El inverso equivalente del método deductivo, pasando desde lo general a los especifico, fue implementado exhaustivamente dentro del Marco teórico, especialmente en la exposición de los

conceptos informáticos y jurídicos que se desarrollaron a detalle introduciendo los conceptos más generales de la informática y el derecho informática, para luego proceder a profundizar en los detalles más específicos de los mismos.

Método analítico:

Si los métodos anteriores sirvieron para la exposición y exploración de las temáticas fundamentales para este trabajo, el método analítico se utilizó fundamentalmente con el objetivo de hacer una disección de estos términos respecto de sus características más significativas, empleando análisis respecto de la terminología y las concepciones doctrinarias.

Método Comparativo:

El método comparativo fue usado ampliamente en el estudio de las legislaciones extranjeras, sobre las cuales se realizó una evaluación comparada y de contraste con el objetivo de poder realzar sus faltas y sus puntos fuertes respecto de la legislación ecuatoriana; este método se ejercitó especialmente en el análisis comparativo del Código Penal de la Nación, El Código Penal Español, La Ley 1273 y la Ley 21459.

Método Estadístico:

Al ser este un trabajo de investigación extensiva que busca dar un diagnóstico sobre el estado de la legislación penal, es uso del análisis estadístico se volvió indispensable tanto al conseguir la percepción general de los profesionales del derecho respecto de la ley, como al analizar los datos provistos por Fiscalía General del Estado en cuanto respecta a los delitos que tienen en sus bases de datos; datos que por sí solos indican únicamente valores respecto de una variable, por lo cual fue necesario el analizarlos y dar una explicación al comportamiento que para un mejor tratamiento fue llevada a través de medios gráficos que permitieran visualizar la magnitud de los datos en su evolución respecto al tiempo.

5.4 Técnicas empleadas

Encuesta: Se realizo un cuestionario consistente de 5 preguntas, a un total de 30 profesionales de derecho en profesión que se relacionaran con la problemática planteada.

Entrevista: Las entrevistas se realizaron a 7 profesionales altamente calificados en cuestiones relacionadas al derecho penal e informático.

Estudio de casos: Al ser este un estudio legislativo, es importante comprobar sus efectos y revisar sus antecedentes, por lo mismo, se hizo uso de un estudio de 3 casos relacionados a la temática de delitos informáticos, mismo que son prueba viva respecto del comportamiento de la norma dictada

cuando esta es llevada a la practica en los tribunales, ya sea de la república, o en el extranjero.

6. Resultados

6.1 Resultados de las encuestas y entrevistas

La presenta encuesta cuenta con 5 literales, las cuales se requirió una respuesta de Si y No, y se les requirió una explicación que reflejara su punto de vista. La población a la que se le realizo esta encuesta consistió en profesionales del derecho de libre ejercicio y funcionarios públicos especializados en derecho, de la ciudad de Loja, Cantón Loja.

6.1.1 Tabulación de Resultados:

1. ¿Estima usted que la legislación penal vigente en términos informáticos es suficiente y ofrece los mecanismos procesales y tipos adecuados para la persecución del fenómeno de la ciberdelincuencia?

SI ( ) NO ( )

¿Por qué?

Indicadores	Variables	Porcentaje
Si	**2**	**6,6%**
90%	**28**	**93.3%**
Total	**30**	**100%**

Tabla 1. Pregunta 1

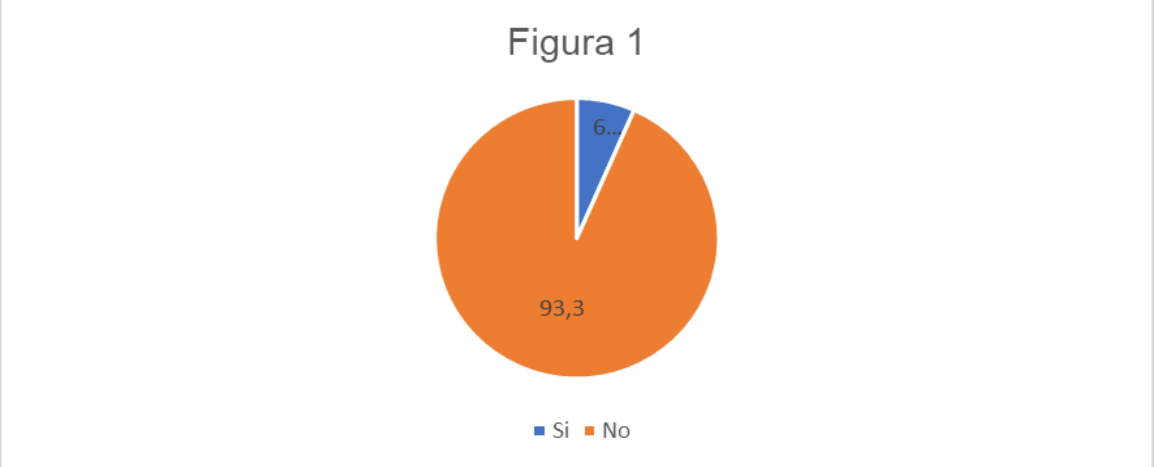

Ilustración 1. Pregunta 1

Fuente: Profesionales de Derecho de la ciudad de Loja

Autor: Joe Sebastián Contento Martínez

Interpretación

En esta pregunta, el 93,3% de los encuestados profesionales de derechos parecen marcar una posición sólida y respondió No, expresando que la legislación penal vigente es insuficiente y no tiene los mecanismos adecuados. Por otro lado, el 6,3%, una minoría estimo que el estado de la legislación le ofrece los mecanismos necesarios y los tipos adecuados.

Análisis

Sobre estos pronunciamientos, los profesionales que se expresaron en contra han puesto sobre la mesa diferentes puntos de vista sobre el por qué estiman la legislación penal actual, insuficiente. Entre estos puntos se encuentran extendidos de manera repetida la perspectiva de una norma atrasada, no adecuada a la tecnología y a los tiempos, teniendo presente la disparidad en la evolución derecho-tecnología, o que de plano sufre de anomias, falta de mecanismos de su aplicación o sanciones inadecuadas, procesos confusos, engorrosos, y dificultades probatorias. Otra opinión recurrente se refiere a la falta de recursos, tanto en material humano calificado, en cuanto respecta a los agentes fiscales y a los peritos, que es el más preocupante; como de recursos que garanticen la aplicación de las leyes.

Por otra parte, los profesionales que se pronunciaron de manera afirmativa concluyen mayormente que la tipificación en el Código Orgánico Integral Penal ha sido clara y ha determinado adecuadamente los mecanismos de procesamiento.

La posición de quien subscribe este trabajo se alinea con la posición del no. Si bien es cierto, existen los tipos dentro del Código Orgánico Integral Penal respecto del tratamiento de ciertos delitos informáticos, una mezcla de falta de capacitación, falta de recursos económicos, desconocimiento de los procesos por parte de la población general, e incluso propios conocedores del derecho, dejan en claro que lo establecido en la norma es insuficiente para perseguir la ciberdelincuencia.

2. En base sobre su experiencia en el campo ¿estima que en ordenamiento jurídico actual es practico y procesalmente viable perseguir acciones informáticas que se desarrollaron en las redes?

SI ( ) NO ( )

¿Por qué?

Indicadores	Variables	Porcentaje

Si	**11**	**36,6%**
No	**19**	**63,3%**
Total	**30**	**100%**

Tabla 2. Pregunta 2

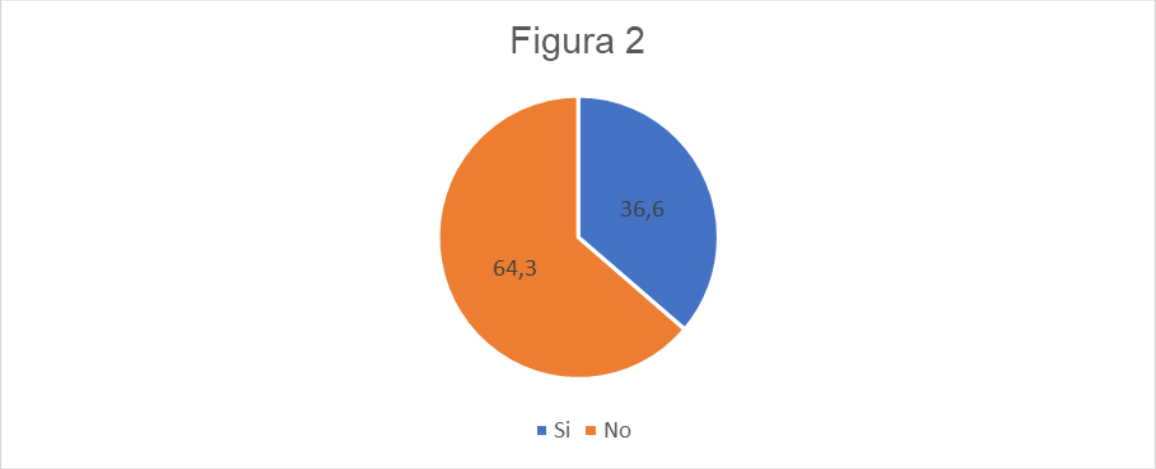

Ilustración 2. Pregunta 2

Fuente: Profesionales de Derecho de la ciudad de Loja

Autor: Joe Sebastián Contento Martínez

Interpretación

En esta pregunta, el 64,3% de los encuestados profesionales de derechos parecen marcar una posición sólida y respondió No, indicando que no es practico, ni viable el perseguir acciones legales, esta posición es coherente con el porcentaje reflejado en la pregunta anterior, pues si no hay mecanismos y tipos adecuados, lógicamente la viabilidad de la prosecución de una acción contra delito informático es reducida. Por otro lado, la minoría aumento en porcentaje con relación a la pregunta anterior, representando el 36,6%.

Análisis

Las pronunciaciones afirmativas negativas mantienen las dificultades derivadas de la pregunta anterior, escasez en formación de personal capacitados, anomias, dificultades probatorias sobre el acceso y serias dificultades en la comprobación de la autoría. Otra que se ha manifestado es precario rendimiento por parte de fiscalía, y no son económicamente viables a consecuencia de la dificultad de poder conseguir un resultado favorable.

Por otro lado, los que se manifestaron en contra lo hicieron con el entendimiento de que la abundancia de casos y el avance de la tecnología, ofrecían un campo propicio, debido a su cada vez mayor relevancia, para su persecución y su propio beneficio como profesionales, es decir,

desde una perspectiva potencial profesional para poder perseguir los delitos, en expectativa de beneficio económico. Otras personas se manifestaron respecto de que aun en la falta norma específica, los términos actuales jurídicos permitían que los abogados pudieran enmarcar los delitos que se desarrollan online, con especial énfasis en las redes sociales, las cuales se refieren que no importa sean libres, no son inexpugnables del todo en cuanto a la responsabilidad de los que ahí cometen infracciones informáticas, además que de estas se pueden recolectar muchos medios probatorios, y argumentan que pese a la dificultad sean pueden rastrear e identificar a las personas, aunque esta no sea exactamente un situación común, argumento que ciertos profesionales reconocen a pesar de pronunciarse afirmativos.

La posición de quien subscribe respecto a este tema se alinea en este caso con la mayoría, y esta posición es consecuente incluso con la tomada en el ítem primero del cuestionario, coincidiendo con el entendimiento de que la legislación penal tiene carencias respecto del manejo de ciertas cuestiones relacionadas al derecho informático. No se puede negar la existencia de tipos vigentes en el Código Orgánico Integral Penal, no obstante, los mecanismos de aplicación, y el retraso en la capacitación del recurso humano en el tratamiento y manejo de medios probatorios, sumado al desconocimiento social sobre estas protecciones y procesos que le otorga la ley, expone un papel preventivo precario de la norma penal informática, y refleja tanto una carencia media en términos de norma, como un carencia severa en términos de manejo de proceso, mecanismos procesales y medios probatorios.

3. ¿Aprecia conveniente a los intereses del Ecuador el adoptar marcos internacionales como mecanismo para modernizar su legislación en cibercriminalidad y delitos informáticos?

SI ( ) NO ( )

¿Por qué?

Indicadores	Variables	Porcentaje
Si	**27**	**90%**
No	**3**	**10%**
Total	**30**	**100%**

Tabla 3. Pregunta 3

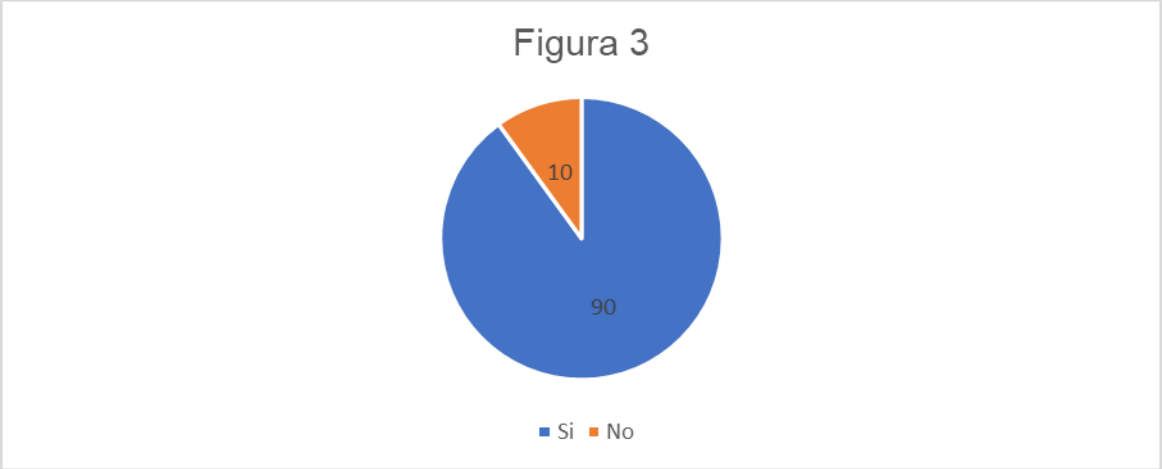

Ilustración 3. Pregunta 3

Fuente: Profesionales de Derecho de la ciudad de Loja

Autor: Joe Sebastián Contento Martínez

Interpretación

Los profesionales se pronunciaron mayoritariamente en favor del Si en esta pregunta, constituyéndose en un 90%, una posición solida que concuerda con la mayoría en los puntos anteriores, pues la percepción de insuficiencia en los mecanismos y tipos jurídicos se ven acompañados de una posición a favor de la adopción de marcos macro estatales para suplirlos. La minoría, se pronunció, No, en un porcentaje correspondiente al 10%.

Análisis

Las respuestas afirmativas sobre este apartado son considerablemente homogéneas: la experiencia extranjera de países más desarrollados, la cooperación internacional y los acuerdos macro estatales, resultaran beneficiosos para tratar poner al Ecuador a la vanguardia de los procedimientos de tratamiento acerca delitos informáticos, donde se podrá obtener avances tanto en los tipos comunes manejados, así como los procedimientos de manejo y operación de las fuerzas de ley.

Las respuestas negativas se explican en posiciones relacionadas con la consideración de que los procedimientos y el material humano ecuatoriano está completamente a la altura de los estándares internacionales, y que, por tanto, no es necesario, no necesariamente perjudicial, la incorporación del estado ecuatoriano a estos estos marcos macro estatales. Otras opciones observan su posición desde las particularidades del contexto ecuatoriano, y la apreciación de que los marcos actuarían sin conocimiento de este, siendo una norma fuera del contexto de la realidad ecuatoriana.

La posición de quien subscribe este trabajo se alinea con la posición afirmativa, esto debido fundamentalmente al valor indispensable que tiene este trabajo respecto de la incorporación de la República del Ecuador al Convenio de Cibercriminalidad de Budapest, el cual estima como de invaluable beneficio para los protocolos de procesamiento penal adecuados al respecto del derecho penal informático.

4. ¿Estima usted que el marco jurídico informático actual protege adecuadamente los bienes jurídicos de la privacidad, seguridad y justicia que garantiza la CRE?

SI ( ) NO ( )

¿Por qué?

Indicadores	Variables	Porcentaje
Si	**4**	**13,3%**
No	**26**	**86,6%**
Total	**30**	**100%**

Tabla 4. Pregunta 4

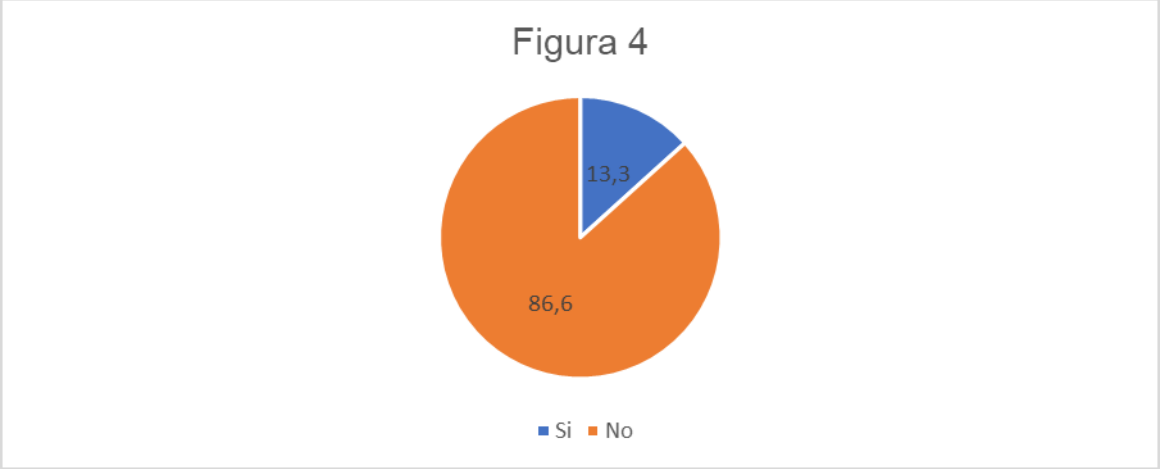

Ilustración 4. Pregunta 4

Fuente: Profesionales de Derecho de la ciudad de Loja

Autor: Joe Sebastián Contento Martínez

Interpretación

Los profesionales encuestados se pronunciaron de la siguiente manera, un 86,6% de los encuestados por el "No"; por otro lado, un 13,3% de los encuestados se pronunció "Si".

Análisis

Los encuestados que se pronunciaron en favor del "No" argumentaron razones relacionadas particularmente a la falta de garantías, mecanismos, reglamentación, las características intrusivas

de la red, dificultades probatorias, falta de socialización de norma, el desface norma-tecnología, y así los factores que aquejan al derecho informático se repiten de manera generalizada en la población muestra.

La población que se ha manifestado favorable respecto de la pregunta se ha expresado entendiendo que los bienes jurídicos mencionados están protegidos por el hecho de existir la norma que desarrolla dicha protección, sin necesariamente analizar sobre las dificultades para aplicar estos desarrollos, no obstante, una de las posiciones estima necesario un aumento en la seguridad y en la normativa, quizá atendiendo a estas falencias prácticas.

La opinión de quien realiza este trabajo se alinea con la opinión de la mayoría nuevamente, argumentando que si bien no se puede negar que existen normativas y políticas que buscan desarrollar las garantías de los bienes mencionados, lo cierto es que cuando viene a la aplicación de estas y, por lo tanto, la consecuente protección de los mencionados bienes jurídicos, la norma y los recursos operativos de las fuerzas del orden se ven insuficiente. Esto se agravia especialmente cuando sumado a las anteriores características, superponemos la misma dinámica en un escenario digital, puesto que, en el ámbito digital, las carencias en norma y operatividad se ven severamente agravadas por la falta de capacitación y las barreras de las jurisdicciones extranjeras.

5. ¿Considera que el Gobierno central ha aplicado una política pública criminal que haya aplacado o disminuido los delitos informáticos y la cibercriminalidad?

SI ( ) NO ()

¿Por qué?

Indicadores	Variables	Porcentaje
Si	**2**	**6,6%**
No	**28**	**93,3%**
Total	**30**	**100%**

Tabla 5. Pregunta 5

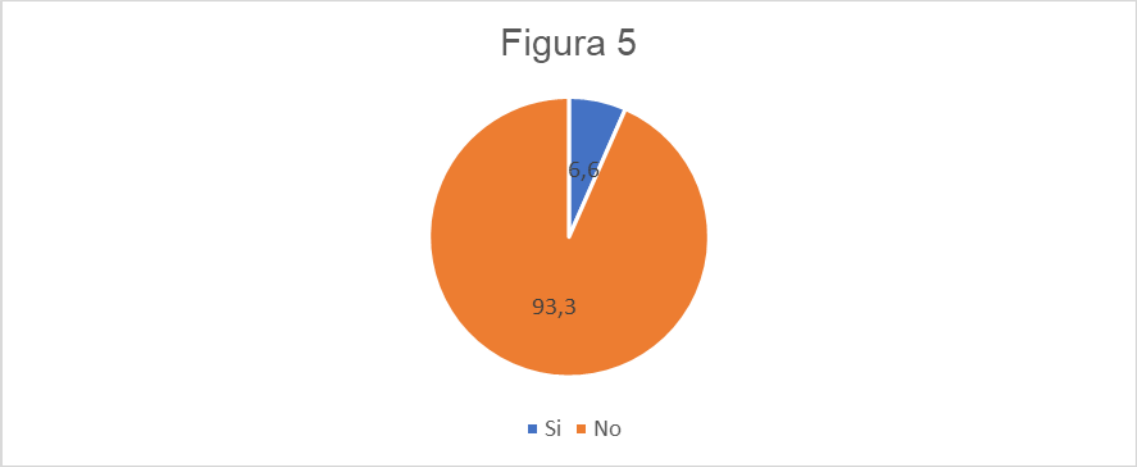

Ilustración 5. Pregunta 5

Fuente: Profesionales de Derecho de la ciudad de Loja

Autor: Joe Sebastián Contento Martínez

Interpretación

Los profesionales encuestados se pronunciaron de la siguiente manera, un 93,3% de los encuestados por el "No"; por otro lado, un 6,6% de los encuestados se pronunció "Si".

La mayoría, abrumadora cabe menciona, se ha pronunciado en favor del "No", apreciando que la política pública por parte del gobierno central es inexistente, insuficiente, ineficiente, desactualizada, débil, deliberadamente corrupta y en el caso de existir, invisible a los ojos de la ciudadanía.

Análisis

Las únicas opiniones en contrario respecto de esta pregunta, aquella que corresponde al 6,6% del total, señala que existen políticas aplicadas por el gobierno central, que se evidencian a través de los portales web, en temas relacionados a la autoprotección de los datos.

La percepción pública, por lo que se observa en los resultados, parece haberse moldeado respecto de la opinión que los sujetos tienen hacia la administración del gobierno central. Existe un criterio mayoritario que indica ampliamente que el gobierno no solo no tiene un rol dentro de la prevención del delito informático a traes de las políticas públicas, además saca tajada al respecto. Este es un punto de vista que se podría considerar sesgado respecto al origen, pero no frente a los hechos, ya que la contundente mayoría expreso no haber visto en todos estos años, ni una sola campaña de concientización activa del gobierno al respecto de este fenómeno, así como tampoco han evidenciado controles o mecanismos disuasivos. Esta opinión, tiene un sustento real, ya que

aun aquellas personas que respondieron afirmativamente se pronunciaron al respecto de que la información se encontraba en portales web de gobierno. Es decir, el único esfuerzo de campaña en contra de este fenómeno tiene un origen de alcance mínimo, baja visibilidad y poco impacto; resultando en una precaria situación de seguridad informática por parte de los ciudadanos, que se agrava sustancialmente cuando consideramos los problemas que surgieron a raíz del COVID, el encierro y la desinformación informática.

6.1.2 Tabulación de las Entrevistas

1. **¿Qué opinión le merece usted el estado actual de la legislación penal informática tipifica dentro del Código Orgánico Integral Penal?**

Respuestas

Entrevistado 1

Dentro del Ecuador están estipulados los delitos informáticos en el Código Orgánico Integral Penal, y me parece que están bien construidos y estipulados, sin embargo, la falta de conocimiento que hay dentro de la ciudadanía, no permite su correcta aplicación, sin embargo, me parece que falta un poco de divulgación, y concientización en la gente sobre la existencia de estos delitos.

Entrevistado 2

Bueno me parece que la tipificación de tipologías relacionadas con los delitos informáticos ha ido evolucionando de manera interesante. En un principio, estas infracciones estuvieron incorporadas dentro de la ley de comercio electrónico, firmas y mensajes de datos, históricamente esa ha sido, hasta 2014 en la cual se derogo, se reformo en materia penal, se reformo este apartado, se derogo el capítulo relacionado con infracciones informáticas, de tal manera que, que cuando se derogo el código penal y el código de procedimiento penal, y entro en vigencia en 2014, el Código Orgánico Integral Penal, entraran en vigencia algunas tipologías que estaban ya recogidas dentro de Ley de comercio electrónico, firmas y mensajes de datos. En todo caso, me parece que es interesante la evolución que ha tenido, porque en nuestro país, a raíz de la última reforma que fue en 2021, se promovieron o se incorporaron en el Código Orgánico Integral Penal, nuevas tipologías relacionadas, por ejemplo, con el ciberacoso escolar, académico, el acoso sexual, el ciberacoso

El grooming ya estuvo considerado en el Código Orgánico Integral Penal desde la vigencia, en 2014, si uno revisa el desarrollo histórico del Código Orgánico Integral Penal, desde 2014, el

173 del Código Orgánico Integral Penal ya regulaba, ya regulaba, este delito, o esta conducta relacionada con el grooming que es el acercamiento de personas suplantando la identidad para acercarse a menores, por medios electrónicos con una finalidad sexual. Entonces esa, básicamente, no es una reforma que se introdujo ahora en Agosto de 2021 en la que si entraron en vigencia, otras tipologías relacionadas sobre todo con la violencia digital, que de alguna manera ya desarrolladas en la Ley para prevenir y erradicar la violencia contra la mujer, a través de la violencia, la violencia digital, cuando uno revisa el artículo 10 de la Ley para prevenir y erradicar la violencia contra la mujer, se encuentra una seria de violencias relacionadas con una violencia psicológica, con la violencia simbólica, y que ahora, en agosto de 2021, se incorporaron como tipos penales que sancionan la violencia dentro del núcleo familiar, violencia familiar, y que está asociada con la violencia digital, prácticas como esa relación de poder, esa relación de dominación por ejemplo, pedirle, solicitarle a la pareja o cónyuge la ubicación, contraseñas, etcétera; se asocia con un tipo de violencia digital, violencia simbólica, electrónica que puede desencadenar en muchos casos, en feminicidios por ejemplo, que son cuestiones que pueden ir agravando, diversos tipos penales u otros tipos penales relacionados con delitos informáticos.

Entrevistado 3

En cuanto a los delitos que se relacionan con el tema informático, el Código Orgánico Integral Penal en la primera instancia establecía infracciones como un tema novedoso que tuvo su primera manifestación en algunas reformas del Código Penal, que estuvieron vigentes el 9 de agosto del 2014. Realiza una serie de tipificación de conductas como delito que tienen relación con los delitos cibernéticos.

Sin embargo, el hecho de que, los sistemas informáticos, los recursos tecnológicos y en sí la tecnología actualmente avance mucho más que cualquier otra ciencia. Hace que cada una de las diferentes conductas descritas en la ley en poco tiempo queden obsoletas. Y así se ha ido dando desde como manifesté desde que se entró en vigor en el 2014 el Código Orgánico Cultural Penal se han venido dando una que otra reforma que datan de ya de algunos meses posteriores a la vigencia del 30 de octubre de 2014. Posteriormente, los mismos seis, y otras reformas de las que ha sido creado el Código Orgánico Integral Penal.

Sin embargo, esto resulta insuficiente. Los tipos penales son inexactos, sobre todo para una ciencia tan avanzada y delicada y que actualmente es utilizada para realizar una serie de conductas ilegales. Entonces, es un tema que sí, siempre debe estar sobre la mesa de discusión y siempre debe

tratar el legislador de ir a la par con los avances de la tecnología y los alcances que puede tener la ciberdelincuencia que, en otros países obviamente más avanzados, tiene un tratamiento mucho más directo, más exacto.

Entrevistado 4

Considero que el legislador está haciendo muchos esfuerzos como para poder manejar, controlar conductas que se dan a través del sistema informático. Pero el avance de la tecnología muchas veces va más adelante que las secciones de reformas y actualizaciones de control punitivo del Estado.

Entrevistado 5

En líneas generales, el Ecuador no ha suscrito el convenio de Budapest de delitos de ciberdelincuencia. Ese documento es no solamente la parte objetiva de tipos penales, sino también procesal y de colaboración internacional. Esa es una gran debilidad por cuanto hoy por hoy los delitos que se cometen online o a través de dispositivos tecnológicos, computadoras, celulares y nuevas tecnologías de la información van en crecimiento potencial por la interacción que tiene el ser humano a través de estos dispositivos. La legislación penal no se ha actualizado acorde con estos convenios y obviamente es una falencia que existe en el tema penal.

Entrevistado 6

Conforme a la dialéctica al igual que la sociedad el derecho viene sufriendo cambios constantes lo que implica que la legislación penal informática también tiene que actualizarse para lograr resultados efectivos para la sociedad,

Entrevistado 7

Justamente hacía mención de que existe materia o normativa respecto a lo que es la parte informática, todo esto no se conoce, con excepción de las partes judiciales, esto lo digo pues en mi experiencia me ha tocado trabajar con abogados y fiscales. Muchos de ellos, ignoran un poco, o no tienen familiaridad del proceso en un ámbito técnico. Por poner un ejemplo, dentro de nuestro campo tenemos un completo proceso técnico para poder dar validez a la prueba, y no hablo de cosas como cadena de custodia, sino algo más intrínseco. Dentro de nuestra especialidad, al trabajar con estándares internacionales como el ISO, se especifican que se deben cumplir con ciertas condiciones para que la prueba sea fehaciente. Esto es que la prueba sea reproducible, verificable, auditable, confidencial e integra. Para lograr esto hay todo un proceso que se sigue, un proceso que la parte judicial no esta tan relacionada o enfocada. En mi experiencia me he tocado con procesos

que no están acorde al proceso técnico, pero que de alguna manera son validados. Y lo mismo ha sucedido a la inversa, procesos técnicamente correctos, pero no son aceptados por falta de conocimiento a profundidad respecto del tema. Entonces sí creo que hay normativa y legislación, pero la capacitación del aparato judicial queda pendiente.

Entrevistado 8

En mi opinión, la legislación penal vigente en términos informáticos no es completamente suficiente y no siempre ofrece los mecanismos procesales y tipos adecuados para la persecución del fenómeno de la ciberdelincuencia.

En primer lugar, la legislación penal puede no estar actualizada para abordar las nuevas formas de ciberdelincuencia que surgen constantemente. Por ejemplo, algunos delitos como la suplantación de identidad en línea o la propagación de malware pueden no estar claramente definidos o penados en las leyes existentes.

En segundo lugar, la ciberdelincuencia es un fenómeno transnacional, lo que significa que los delincuentes pueden actuar desde un país y afectar a víctimas en otro. Esto puede plantear desafíos en términos de la aplicación de la ley y la jurisdicción. En algunos casos, la legislación de un país puede no permitir la persecución de delitos cometidos fuera de sus fronteras.

Además, la ciberdelincuencia puede ser más difícil de investigar y perseguir que los delitos convencionales, ya que los delincuentes pueden ocultar su identidad o usar tecnologías avanzadas para ocultar sus actividades. Esto puede dificultar la recolección de pruebas y la identificación de los responsables.

En resumen, aunque se han implementado leyes específicas para abordar la ciberdelincuencia, estas pueden no ser suficientes para abordar todas las formas de ciberdelincuencia. Además, los desafíos de la ciberdelincuencia en términos de jurisdicción y recolección de pruebas pueden dificultar la persecución efectiva de los delitos en línea.

Entrevistado 9

Por supuesto, como abogado, considero que la legislación penal informática tipificada dentro del Código Orgánico Integral Penal es un avance significativo en la lucha contra la ciberdelincuencia en Ecuador. El Código Orgánico Integral Penal establece una serie de tipos penales específicos que se refieren a la comisión de delitos informáticos, lo que permite a los operadores jurídicos contar con herramientas legales claras para investigar y enjuiciar estos delitos. Aunque siempre habrá espacio para mejoras y actualizaciones, el Código Orgánico Integral Penal

representa un paso importante en la lucha contra la ciberdelincuencia.

Entrevistado 10

A mi parecer los términos penales vigentes en cuanto refieren a delitos informáticos en Ecuador es adecuada, pero todavía hay espacio para mejorarla. Aunque la legislación actual incluye delitos informáticos, como la violación de sistemas, la interferencia ilegal en sistemas informáticos y la difusión de virus informáticos, todavía hay ciertas áreas en las que se necesita mejorar la protección de los usuarios de Internet y las empresas que operan en línea.

Por ejemplo, los delitos informáticos en la actualidad están regulados en el Código Penal, pero se pueden presentar ciertas dificultades en la investigación y persecución de estos delitos. Esto se debe a que muchos de los delitos informáticos son transnacionales y las autoridades nacionales no siempre tienen las herramientas adecuadas para trabajar con otros países y perseguir a los delincuentes.

Otro desafío que enfrenta la legislación penal en términos informáticos es la necesidad de actualización constante para hacer frente a las nuevas formas de delitos que surgen constantemente en la era digital. Por lo tanto, la legislación debe estar en constante evolución para hacer frente a los delitos informáticos que pueden surgir.

En resumen, aunque la legislación penal vigente en términos informáticos en Ecuador es adecuada, todavía hay margen para mejorar y adaptarla a los cambios tecnológicos constantes y a la complejidad del mundo digital actual.

Comentario del autor

El criterio de entrevistador respecto de las respuestas de los entrevistados es uno de concordancia con lo expresado. Los entrevistados en términos muy generales reconocen un avance en a la legislación penal local, indicando esfuerzos de la ley penal y valorando que a pesar de estas mejoras existen serios problemas derivados de las capacidades operativas y de material humano de la fiscalía general del estado. En especial, concuerdo en totalidad con la posición expresada por el tercer y quinto entrevistados, el primero en su expresión de las inadecuaciones pendientes del Código Orgánico Integral Penal; y el segundo sus preocupaciones derivadas de la adhesión del Ecuador en el Convenio de Cibercriminalidad de Budapest, derivando en tipos que no son fácilmente adaptables en el momento de cooperar internacionalmente.

2. ¿Encuentra que los mecanismos de persecución formalmente configurados en el

ordenamiento actual son procesalmente eficientes y eficaces?

Entrevistado 1

Como le decía hay la falta de conocimiento por parte de la sociedad, para que las personas las cuales se han vulnerado los derechos por medio de estos delitos informáticos sepan que existe este respaldo que pueden encontrar en el Código Orgánico Integral Penal, para aplicar la normativa correspondiente y no se repitan.

Entrevistado 2

Bueno, esta es una interesante pregunta ¿si son eficaces? Porque, la eficacia, si uno mide o analiza el termino eficacia con la relación de disminución de delitos informáticos yo creo más bien, propósito incluso de la emergencia sanitaria o del uso de medios tecnológicos, esta situación de delitos informáticos o de delitos digitales, se han ido agravando, se ha indo agrando la verdad.

Entonces, en materia penal es muy difícil establecer cuestiones relacionadas con eficacia. La eficacia, evidentemente de una norma, sea en el ámbito civil, en el ámbito penal, en el ámbito laboral, en cualquiera de las áreas de derecho, tendría que estar relacionada evidentemente con la disminución ¿verdad? O que se yo con, por ejemplo, en el ámbito constitucional con cuestiones de transparencia, con cuestiones de acceso a la información, etc.

Pero vemos que estas cuestiones se van gravando, van empeorando, entonces hay que ser consciente que el ámbito penal, muchos tipos penales no solamente relacionados con delitos informáticos, no se han disminuido, sino se han agravado, entonces la solución no es que de pronto, contar con una legislación, o el mayor catálogo de normas que sancionen delitos informáticos, ayuda a disminuir o contrarrestar delitos relacionados con, este caso, delitos informáticos.

El problema de la eficacia se debe medir, evidentemente, por cuestiones sociales. No por el hecho de contemplar normas, tener normas que sanciones delitos informáticos, sí, es necesario contar con un marco regulador atendiendo el principio de tipicidad, sabemos que en el derecho penal juega un papel muy importante, principio de tipicidad, es decir se sancionan aquellas normas que están previamente tipificadas, principio de legalidad, de tipicidad; pero, evidentemente, pues hay que decirlo, que la eficacia no se la puede medir únicamente por el hecho de contar con tipos penales dentro de la legislación, hay otras cuestiones que son vinculantes a este problema y ahí hay que hablar mucho sobre la cuestión de la corresponsabilidad.

¿La corresponsabilidad que implica? El principio de corresponsabilidad implica, el papel que debe cumplir no solamente el Estado, a través de la promulgación de normas, el Estado a través

de la Asamblea Nacional con la promulgación de leyes o de normas; sino también juega un papel muy importante la sociedad y la familia. Entonces hay muchos delitos informáticos que se desprenden del desconocimiento, mucha gente que cree que internet, que las redes sociales son espacios impunes, que no es así, se comparte mucha información personal, mucha información intima, tenemos que, el hecho cuando uno recibe un video, por ejemplo, intimo, de una tercera persona y vulnera su intimidad, su privacidad, creemos que volver a compartir ese video no ocasiona ningún prejuicio, o no se está cometiendo ningún tipo de ilícito. Y aquí, revisando, por ejemplo, el 178 del Código Orgánico Integral Penal, que es el delito de violación a la intimidad, es tan responsable la persona que comparte por primera ocasión como la que vuelve a difundir, y la vuelve a compartir, y la vuelve a compartir.

Esa sería la percepción de eficacia, una eficacia que no debería estar solamente vinculada a ser efectivo el control social y control estatal, sino también esa labor que se debe cumplir, esa labor que se debe desarrollar desde la sociedad y la familia para prevenir, porque evidentemente a partir de uno de los principios de materia penal, el ejercicio de este poder punitivo del estado a través de la normativa penal, se lo debe ejercer de ultima ratio, en última instancia, ya cuando se han agotado otros mecanismos, esos mecanismos están relacionados, evidentemente, con la prevención.

Evidentemente las políticas púbicas también pueden ayudar a contrarrestar, a prevenir, pero seguimos en el mismo juego de estimar, si son efectivas o no son efectivas por ejemplo, determinadas políticas para prevenir delitos informáticos, hay una política pública del consejo nacional para la igualada intergeneracional que es la política pública para resguardar la integridad de los menores en internet, entonces esta política pública fue promulgada en 2021, y hay que ver cuantas instituciones educativas, cuantas instituciones no solamente público, en el ámbito privado, tienen conocimiento de la vigencia de esta norma, no desde esta norma, de esta política, que a larga son normas que están destinada a prevenir, a erradicar la violencia digital, la violencia electrónica y prevenir una serie de delitos relacionados con la informática.

Entrevistado 3

Tenemos inconvenientes graves. Las herramientas procesales con las que se cuenta en este aspecto suelen no se suficientes. El procedimiento para levantar evidencia digital, le falta desarrollo en el Código Orgánico Integral Penal.

Si bien contamos existen, aquí en Loja particularmente son muy buenos peritos que saben

cómo levantar una evidencia, saben resguardarla, saben de algún modo manejar una cadena de custodia de un elemento que a veces resulta inmaterial. Entonces las herramientas no son suficientes, recursos económicos muchísimo menos. Entonces ahí sí hay un obstáculo para realizar una efectiva investigación y en estos delitos tan nuevos y que siempre están en constante evolución.

Entrevistado 4

Si, entiendo de que, en realidad, así como la informática va desarrollándose de un día a otro, el sistema jurídico y también profesional de los que estamos operando, también se reforma. Si hay un desfase en el desarrollo de la tecnología, se podrían aprovechar organizaciones y violentar el sistema legal en el que estamos.

La ley tiene que ir desarrollándose al mismo paso de la tecnología. Sin embargo, la tendencia es que va ganando, va adelantada la situación informática. Cambia de un momento al otro y la situación legal no es que de un momento al otro va a cambiar, sino que necesita también la aprobación de reformas que ya sabemos que son parte del sistema operativo.

Entrevista 5:

No podrían ser eficaces en el tema de delitos informáticos. Porque, por ejemplo, si te requiere la determinación de algún delito de sexting, phishing o cometidos a través de redes sociales como WhatsApp o Facebook, como el grooming, por ejemplo, si o grooming, no hay la facilidad de obtener la información desde esas centrales: Facebook, WhatsApp, Instagram. Entonces, los tiempos procesales que están en el código de proceso, el Código Orgánico Integral Penal son muy cortos, si es que ya estamos en una fase de instrucción fiscal. Hay que considerar que dependiendo la pena, una investigación previa puede durar un año o máximo dos, tiempo que para el tema de delitos informáticos, sin las debidas coordinaciones internacionales y sin los convenios suscritos de cooperación internacional con otras fiscalías a través del convenio marco, que es el de Ciberdelincuencia, se complica la remisión de esa información y cuando no tiene información para verificar la existencia material de la infracción, peor se va a poder determinar quién es el responsable. Considerando que los delitos informáticos se cometen detrás de una pantalla y no se sabe quién es la persona que está detrás de la pantalla.

Entrevistado 6

La legislación penal en lo relacionado a los delitos informáticos, para su persecución, en si por tratarse de conductas utilizando medios tecnológicos y la internet, viene siendo en muchos caso imposible lograr resultados positivos para la víctima, por ejemplo en caso de hurto de dinero en

entidades financieras el delincuente al apoderarse de la clave de la víctima realiza transferencia a una cuenta bancaria, luego realizan a otra cuenta bancaria y finalmente retiran el dinero de otra cuenta bancaria, y como estos movimientos pueden realizarlos incluso desde fuera del país, se torna imposible la recuperación de los dineros sustraídos mediante esta modalidad, esto viene pasando con algunas entidades financieras.

Entrevistado 7

Como peritos, si bien seguimos procesos establecidos, tan solo participamos de una parte del proceso judicial. No manejamos a profundidad normativa relacionada al buen proceso; tenemos conocimiento de algo, pero es mayoritariamente lo que está relacionado con nuestras partes. A mi opinión, con lo que hemos tenido ha sido más que suficiente, aunque debo admitir que desconozco si existían más normativas o procesos que se puedo haber seguido. Sin embargo, con lo que ha habido se pudo desarrollar las actividades con normalidad.

Entrevistado 8

En general, los mecanismos de persecución formalmente configurados en el ordenamiento actual pueden ser eficientes y eficaces, siempre y cuando se apliquen correctamente y se les proporcione los recursos adecuados.

En Ecuador, el sistema de justicia penal ha experimentado cambios importantes en los últimos años, incluida la implementación del Código Orgánico de la Función Judicial y la creación de la Unidad de Investigación de Delitos Informáticos. Estos cambios han mejorado la capacidad del sistema judicial para investigar y procesar delitos informáticos.

Sin embargo, como en cualquier sistema legal, hay desafíos que enfrentar. Por ejemplo, la falta de recursos y capacitación especializada puede ser un obstáculo para la eficacia del proceso de persecución en casos de delitos informáticos. Además, la complejidad de los casos de delitos informáticos y su carácter transnacional pueden dificultar la identificación y el enjuiciamiento de los delincuentes.

En resumen, si bien los mecanismos de persecución formalmente configurados en el ordenamiento actual pueden ser eficientes y eficaces, se requiere una aplicación adecuada y la asignación de recursos y capacitación especializada para enfrentar los desafíos que surgen en el contexto de los delitos informáticos.

Entrevistado 9

Yo considero que los mecanismos de persecución formalmente configurados en el

ordenamiento actual para la lucha contra los delitos informáticos son eficientes y eficaces, siempre y cuando se apliquen correctamente. El Código Orgánico Integral Penal establece procedimientos específicos para la investigación, enjuiciamiento y sanción de los delitos informáticos. Sin embargo, la eficacia y eficiencia en la persecución de estos delitos dependen también de la capacidad de las autoridades competentes para aplicar estos mecanismos de manera adecuada, así como de los recursos disponibles para llevar a cabo investigaciones exhaustivas y complejas. Por tanto, es importante seguir trabajando en el fortalecimiento de los mecanismos de persecución y en la capacitación del personal encargado de su aplicación.

Entrevistado 10

En mi opinión como abogado, los mecanismos de persecución formalmente configurados en el ordenamiento actual para los delitos informáticos tienen ciertas limitaciones en cuanto a su eficiencia y eficacia procesal. Aunque existen tipos penales específicos en la legislación y se han establecido procedimientos específicos para el tratamiento de estos delitos, todavía hay una falta de capacitación en las instituciones encargadas de la persecución y juzgamiento de estos delitos. También es necesario abordar la complejidad técnica de algunos delitos informáticos, lo que puede generar dificultades para recolectar pruebas y, en consecuencia, afectar la eficiencia procesal.

Comentario del autor

Mi opinión respecto de las respuestas expresadas en la segunda pregunta, expreso parcial concordancia con la opinión de los expresados por los entrevistados. La segunda pregunta tenía como propósito encontrar respuestas respecto de la realidad procesal de los tipos descritos en el Código Orgánico Integral Penal, para a través de la valoración de quienes hacen un uso procesal de estos tipos, se pudiera evidenciar el impacto que tiene este y el estado que tienen estos tipos en el sistema judicial de justicia. Las perspectivas que se ofrecieron abarcaron un estado de desconocimiento y falta de socialización con los ciudadanos que tiene como consecuencia una reducida persecución de estos actos punibles; encuentro esta posición un argumento crucial cuando respecto de la eficacia de la ley se trata. Como expone el segundo entrevistado, la noción de la existencia de una norma en el pensamiento general de la población es determinante para su ejercicio, puesto que si bien la fiscalía tiene la capacidad de actuar de oficio, es a través de la denuncia particular donde se da el origen de la gran mayoría de los procesos que se impulsan en el sistema judicial; el desconocimiento tiene entonces como resultado una reducción sustancial en las denuncias, y por lo tanto, las actividades delictivas proliferan en la impunidad. Respecto de esta

perspectiva mi opinión es favorable, no obstante, debo reconocer que la responsabilidad esta falta de socialización no se le puede atribuir al Código, siendo una consecuencia directa de la falta de campañas de concientización e información que están en potestad del Gobierno nacional a través de las políticas públicos. Quiero además hacer mención sobre la posición emitida por el quinto entrevistado, donde este se pronuncia respecto de los problemas procesales derivados de transnacionalidad de los delitos, una noción ignorada por la norma, que dificulta en considerable proporción la consecución de los datos que actúan como medios probatorios; una opinión que tiene concordancia con la expresada por él sexto entrevistado que expone las dificultades para conseguir resultados cuando los acontecimientos superan las fronteras nacionales, llevando al desistimiento muchas veces por parte de la víctima. Cuestión que a criterio de quien aquí subscribe es fundamental para entender las dificultades de prosecución de las causas en estos delitos.

3. **¿Ha encontrado usted dificultades procesales al momento de encausar un delito con carácter informático? ¿Cuáles fueron estas dificultades?**

Entrevistado 1

Realmente porque me dedico al tema de la academia, y no he tenido la oportunidad de trabajar directamente con la presentación de una denuncia de carácter penal sobre delitos informático, no podría decirle cuales fueron estas dificultades, sin embargo, creo yo que lo más importante que falta ahora es peritos preparados en temas informáticos, ya que lo más importante para poder corroborar y determinar estos delitos es la prueba que se pueda presentar.

Entrevistado 2

Hay muchos delitos, por ejemplo, que han sido publicados o que han sido puesto en conocimientos de la sociedad a través de la página de la Fiscalía General del Estado, aunque ahora a propósito incluso de la emergencia sanitaria, han existido muchos casos de por ejemplo de gromming, muchos casos relacionados con violación a la intimidad, casos relacionados con estafas informáticas, cual es el principal problema, o por ejemplo llamados a extorsionar a través de medios telemáticas, correos electrónicos, fishing, suplantación a la identidad, las variantes del fishing, snitching, catfishing, etc. Pero el problema, los principales problemas, pasan, creería yo, que pasan por el desconocimiento de las autoridades, fiscalía, hay que entender que a los delitos informáticos se pueden promover la prosecución en el ámbito, se puede promover desde el ámbito de un delito de acción pública, o desde el ámbito de un delito acción privada. Entonces hay muchas autoridades que todavía desconocen la naturaleza de estas tipologías, y también las personas desconocen, creen

que de pronto no existen mecanismos legales, no existen herramientas jurídicas, o en el caso de que existan, hay muchos delitos informáticos que están relacionados con la violación a la intimidad o con los fraudes. Entonces acá viene la doctrina, que ha sido muy enfática en de estar que las características que se desprenden de estos delitos informáticos y que están asociadas a la victimología de las personas que sufren estas infracciones, pasan un poco por la vergüenza de denunciar este tipo de ilícitos. ¿A que me refiero con la vergüenza de denunciar este tipo de delitos? Imaginémonos un caso, un supuesto de una violación a la intimidad por medios informáticos, imaginémonos el supuesto de que esta víctima, generalmente las mujeres, acuden con fiscalía a denunciar este tipo de ilícitos, las victimas prefieren no denunciarlo para no ser objeto del escarnio público, es decir, además de que he sido objeto de un delito de violación a la intimidad, una víctima se imagina que va tener que presentar nuevamente sus fotografías, desnudo, semidesnudo, entonces ese escarnio público, representa una limitación para que las personas por ejemplo que han sufrido delitos relacionados con violación a la intimidad no denuncien, por la vergüenza que obviamente tienen que presentar, decir cuáles han sido los antecedentes, la relación circunstancial, muchos delitos están relacionados con eso. Otro delito del que he tenido conocimiento igualmente que han sido víctimas por ejemplo personas, relacionadas con la extorción, por ejemplo, hacen llamadas, la típica llamada suplantando la identidad de familiares, se quedaron varadas en un aeropuerto, y luego llaman solicitar un favor sabes que necesito dinero para sacar la maleta, etc., por favor transfiéreme a tal cuenta o tal cuenta de la aerolínea para que me dejen sacar mis maletas, etc. Yo ya te devuelvo, fingen, suplantan la identidad evidentemente, pero se dejan engañar de este tipo de fraudes informáticos, se dejan engañar, y evidentemente las personas que han sido víctimas y transfieren este dinero, luego prefieren no hacerlo, porque resulta tan sarcástico y hasta cierto punto humillante, decir bueno me deje engañar tan infantilmente que prefiero no hacerlo, decir bueno, ¿cómo lo hiciste? ¿por qué lo hiciste? No tuviste consciencia de pronto que te estaban engañando, que te estaban tratando de apropiarse de tu dinero, etc. Entonces hay muchas cuestiones, trabas procesales, y en primer lugar el desconocimiento de las autoridades por la proliferación de este tipo de ilícito, y luego por la carencia de herramientas en el ámbito procesal para la investigación, y por otro lado obviamente, atendiendo a la victimología de este tipo de infracción, esto está relacionado con la vergüenza que tienen muchas personas para denunciar este tipo de delitos.

Si revisamos, yo creería que no existen dificultades probatorias, si vamos desde el ámbito legal, desde el ámbito normativo, no existen dificultades para poder garantizar que una evidencia

electrónica, pueda servir para demostrar la materialidad de la infracción, y la responsabilidad, el nexo causal, no existe un vació,, no existe ausencia, existe una norma, el número 500 del Código Orgánico Integral Penal, establece la importancia de poder aportar dentro de un escenario judicial evidencia electrónica, evidencia digital, ahí el 554, numeral 4 del Código Orgánico Integral Penal, principios en materia probatoria, que es el principio de libertad probatoria, cual se puede utilizar cualquier tipo de medio de prueba, y eso incluye la evidencia electrónica, la evidencia digital, ¿dónde está el problema? el problema recae nuevamente en la dificultad para poder interpretar y poder garantizar de que efectivamente esa prueba puede servir, no hay un vacío legal, no hay ausencia de norma, incluso si revisamos el código orgánico de la función judicial, también garantiza la aplicación el uso de evidencia electrónica que incluye materia penal, entonces no hay una ausencia de normas, si hay ausencia, y descornamiento, sobre todo en la forma en cómo se debe interpretar, y eso lo ha dejado en claro la doctrina internacional, la doctrina nacional también, que debe haber una justicia especializada tanto como en otros contextos, otros países, fiscalías especializadas sobre ciberdelitos, jueces especializados.

Hubo la aprobación, si mal no recuerdo, en 2022, inicios del 2022, existió la aprobación por la fiscalía general del estado, para que se incorpore a la fiscalía, una fiscalía especializada para la investigación y procesamiento de delitos informáticos, vamos a ver, vamos a cumplir un año, inicialmente esa resolución de la fiscalía general del estado esta para que se cree una fiscalía especial en quito, y se traslade según las necesidades a distintas jurisdicciones, vamos a ver cómo funciona, si a larga pretende ser lo que en esta resolución de la fiscalía dice que entre la fiscalía general del estado y las autoridades competentes para el juzgamiento de este tipo de infracciones, debe haber capacitación, debe haber programas de preparación de fiscalía, de los jueces, etc.; de peritos que puedan coadyuvar para ampliación de los principios que si tenemos en materia penal, lo que pasa es que no hay muchos conocimiento por parte de autoridades, ahora esto implica también reconocer , hay que insistir en esto, la importancia de contar con una justicia especializada, los delitos informáticos son delitos especialmente gravosas que no solamente implica la vulneración de un ben jurídico, sino de varios bienes jurídicos al mismo tiempo, esa es una característica que ha descrito la doctrina, la jurisprudencia internacional, entonces el problema pasa por ahí, evidentemente por la falta de herramientas relacionadas con la capacitación, la preparación de las autoridades, y de una justicia especializada.

Entrevistado 3

Bueno, he tenido algunas infracciones que se las ha judicializado ya por delitos informáticos. El principal obstáculo que hemos tenido es que muchas veces la persona jurídica. En cuyo sistema estudió la interacción, por el mismo hecho del avance de los sistemas había sustituido el sistema anterior, por uno nuevo y el delito fue cometido en el sistema anterior.

Incluso el propio perito encontró dificultad en poder reconstruir esta evidencia digital para poder llegar a una conclusión indudable sobre la responsabilidad del autor. Pero, como digo, gracias a dios, el perito muy entendido en la materia, obviamente, pudo sacar por lo menos la información para responsabilizar, aunque no completa, eso sí debo decirlo.

Y así resulta no solamente en esta institución que era particular, sino también instituciones del Estado, donde para poder dar un poco más de agilidad al servicio, cambian de sistema y los datos anteriores muchas veces se pierden o quedan incompletos y a partir de ahí es la dificultad.

¿Existen herramientas? Sí, en donde usan los teléfonos celulares y se puede recuperar información que ha sido borrada.

Pero el problema son las dificultades económicas del Sistema Nacional de Investigación. En la que, por ejemplo, hay que adquirir licencias para para tener este tipo de software que ayuda a recuperar todas estas situaciones y realmente tenemos, y muchas veces se han truncado investigaciones por esto.

Hay un manual que lo había redactado, un perito, una persona particular sobre el procedimiento exacto de cómo se debe realizar el levantamiento y conservación de evidencia digital, precisamente porque no hay de forma explícita ese proceso. Solamente lo habla de manera muy genérica, no es como cuando habla, por ejemplo, de la recolección de evidencia biológica que de manera muy clara se establece protocolos para hacerlo, y esto se desarrolla a veces en estos tiempos legales, como son protocolos, directrices y demás de los delitos, pero en el caso de sistemas informáticos se sufre un poquito todavía más.

Usted sabe que la persona que está sentada al otro lado de una pantalla realizando. actitudes o actividades, perdón, de índole ilegal. El hecho de que se le solicite a la proveedora de servicios de Internet una dirección vea al nombre de quien está, no es una seguridad para tener la certeza de que la persona que tiene la titularidad de esa IP estuvo accediendo a esa máquina, por ejemplo.

Entonces es difícil esa autoría y por eso hay que recurrir a otras pruebas, aunque sean iniciales, por ejemplo, si la persona que es la propietaria de la IP estuvo con acceso a esa máquina por que digamos es el dueño del equipo. Y se realizó, por decir, un ataque informático a un sistema

para borrar una multa, cuyo titular es él mismo, entonces ahí está el nexo causal y es más fácil. Pero sí hay otras circunstancias (inentendible) es un poquito más difícil. Le pongo un ejemplo.

Yo tuve un caso de peculado, cuyo delito medio fue el ataque de, bueno, no fue la introducción del mismo funcionario público al sistema informático para purgar multas de usuarios que habían sido sancionados mediante boleta de tránsito. Entonces se había realizado una serie de dejar sin efecto sanciones que incluso tenían sentencia condenatoria

Y ¿cómo se determinó que él era? Porque fuimos a su casa. Realizamos un levantamiento, esta ocasión de una máquina de escritorio. Se preservó la evidencia y le comento que fuimos con un perito que es muy bueno, existen dos o tres que son excelentes aquí, y él a través de realizar la búsqueda en los backups o un nombre así, no recuerdo exactamente, determinó que en esa casa, en esa máquina particular se había instalado el software UCOD y que se había navegado dentro desde la casa de este ciudadano al sistema para realizar esas acciones que ya habían sidas borradas el rastro, pero quedaba esa huella que desde esa casa sin tener por qué razón, entrar desde una casa particular, entonces de ahí se ido probando, probando, probando pero no en todos los casos, entonces si existe una dificultad.

Entrevistado 4

Dr. Carrión: Si, esto está relacionado con lo anterior, considero que debe existir la pericia que lo hace el perito no es una de forma calificada y técnica. Es necesario actualizar los medios que nos encontramos en los cuales debe haber más esa capacitación de los peritos, que realizan este tipo de levantamiento de evidencias en el aspecto informático.

Entrevistado 5: La pregunta es orientada más bien a fiscalías en un rol de investigación. En mi calidad de defensor público, yo por la labor que se desempeña en la institución, realizamos actos de defensa en favor del procesado o del investigado, dependiendo la fase en la que se encuentra. Pero en líneas generales, los delitos informáticos han sido escasos en el conocimiento institucional como defensoría pública, entiendo que existe una institución desde la Policía Nacional especializada en temas de investigación de delitos informáticos y desde la Fiscalía también, pero no hay una mayor incidencia estadística formal de presentación de denuncias que nos hagan tener una métrica de cuántas denuncias se han presentado y en qué casos se han resuelto. Esa es una dificultad allá donde el orden operativo.

Entrevistado 6

Claro, por ejemplo, a mi criterio hay un muy mal manejo de la cadena de custodia. En algún

momento tuvimos en análisis informático forense de una cooperativa. Se tomo el equipo con el proceso que corresponde, se obtuvo huellas digitales, les llamamos hash, que son valores únicos para cada recurso digital, y se puso todo a custodia de las autoridades. Sin embargo, posterior a nuestra pericia se ordenó una pericia a cargo de un perito contable, mismo que no tomo los debidos resguardos sobre la información, lo que vendría a ser la cadena de custodia y el proceso para manejar la información de los servidores, resultando como consecuencia que, a causa de esta mala práctica, la prueba quedara invalidada. Este es uno de muchos casos.

En otra ocasión, trabajamos en una pericia fuera de la provincia, y trajimos unos equipos. Estos equipos no siguieron una cadena de custodia adecuada. Se levanto, se inventario, pero no se los entrego como se debía. Unos códigos de serie no coincidían con los equipos.

Entonces, existe descuido y falta de experiencia en el manejo de la información. En otros ámbitos, el trabajo y coordinación con organismos nacionales generan problemas. Algunos casos se dan cuando se tiene que analizar información de sistemas que se encuentran en otros países, veamos Twitter, siendo imposible acceder a esta información localmente, y debiéndose hacerse una gestión a través de organismos internacionales. Para concluir, diría que existen apartados que requieren optimizarse ya que entorpecen el proceso.

Entrevistado 8

Mi experiencia en la temática está limitada exclusivamente a lo que conozco por doctrina, no tengo experiencia personal en la encausación de delitos con carácter informático. Sin embargo, puedo decir que en general, acogiendo las opiniones de mis colegas, los delitos informáticos pueden presentar desafíos procesales que dificultan la encausación de los mismos.

Uno de los desafíos comunes en la encausación de delitos informáticos es la identificación del autor o autores del delito, ya que los delincuentes pueden ocultar su identidad detrás de direcciones IP falsas o utilizar técnicas de anonimización. Además, la naturaleza transnacional de muchos delitos informáticos puede hacer que la jurisdicción y la cooperación internacional sean difíciles de establecer.

Otro desafío es la recolección y el análisis de pruebas digitales, que pueden requerir habilidades especializadas y herramientas de análisis específicas. La falta de capacitación especializada en la recolección y análisis de pruebas digitales puede ser una barrera importante para la encausación exitosa de delitos informáticos.

Entrevista 9

Es común que existan dificultades procesales al momento de encausar un delito con carácter informático, ya que estos delitos suelen involucrar tecnología y redes de comunicación complejas. Algunas dificultades pueden incluir la identificación de los autores, la recolección de pruebas electrónicas y la determinación de la jurisdicción adecuada. Por esta razón, es importante contar con profesionales capacitados y recursos técnicos adecuados para garantizar una adecuada persecución de los delitos informáticos.

Entrevistado 10

Sí, en mi experiencia en el oficio he encontrado dificultades procesales al momento de encausar los delitos que mencionas. Algunas de estas dificultades incluyen la obtención de pruebas suficientes para respaldar la acusación, sobre todo con los peritos actuales, ya que a menudo los delitos informáticos involucran el uso de tecnologías avanzadas que pueden dificultar la recolección de pruebas. También puede haber dificultades en la identificación del autor o autores de los delitos, ya que a menudo se utilizan técnicas de anonimato y suplantación de identidad en línea. Además, existe una falta de capacitación especializada en los encargados de investigar y juzgar estos delitos, lo que puede afectar la calidad de la investigación y el proceso judicial.

Comentario del autor

La tercera pregunta tenía por intención consolidar más detalladamente las dificultades específicas que se experimenta en la persecución de estos delitos, esto puesto que son nociones que dificultan la consecuciones de la justicia, y que son cuestiones que el Código Orgánico Integral Penal no tiene presente en sus términos, que requieren una mayor atención del ejecutivo y legislativo en consecuencia; Esto con objetivo secundario de obtener nociones externas pero reales que puedan aportar para contextualizar las acciones y lineamientos propositivos posteriormente.

El criterio sobre el cual se subscribe el presente trabajo respecto de las opiniones vertidas por los profesionales de derecho entrevistados es uno de preocupación. Los criterios emitidos en mayoría común entre los especialistas, evidencian un problema que no es estrictamente legal, sino uno de recursos humanos dentro del sistema judicial, que si bien no expone una responsabilidad sobre la legislación, supone una afectación sustancial que merece ser elevada a discusión, ya que la ley no es más que una ficción jurídica, a menos que pueda materializarse dentro de la sociedad que busca normar, siendo la poca capacitación o ignorancia de los agentes fiscales, peritos y operativos un factor degenerativo del efecto real de la norma de suma importancia. Como expuso el segundo entrevistado, en una opinión con la que estoy profundamente de acuerdo, no basta

únicamente con contar con el catálogo de delitos informáticos más amplio y completo producido por el ser humano, sino existen los mecanismos procesales y el recurso humano capacitado para poder llevarlo a cabo, siendo así una preocupación personal los manejos del personas investigativo de justicia qué a la luz de las opiniones, y anécdotas como la de la entrevistada tres, pueden fallar e invalidar elementos sustanciales del proceso. Como opinión conclusiva expreso que existe un serio problema no en la legislación, pero existe en los órganos y personal encargados de su aplicación, que, para efectos prácticos, culminan con un mismo resultado, una pobre persecución del delito informático y una escasa consecución de justicia, reparación y conclusión de procesos.

4. **A su criterio personal ¿Que le faltaría implementar o modificar a la política criminal del Gobierno central para combatir y prevenir los delitos informáticos?**

Entrevistado 1

Igualmente, como dije en la primera pregunta, falta socialización de este tipo de delitos. Recordemos que actualmente debido a las nuevas tendencias de la información y de la comunicación hay muchos delitos que se configuran a través del uso de redes sociales, entonces creo yo que, si falta, por medio del gobierno central, igualmente la socialización de que existen leyes, que pocos lo saben, sobre el cometimiento de los delitos informáticos para prevenir la cibercriminalidad.

Entrevistado 2

¿Qué le faltaría? Aparte de las normas que se han ido incorporando progresivamente en materia penal de delitos informáticos, yo creería que hace falta, la aprobación evidentemente del Convenio de Cibercriminalidad de Budapest. Es una norma muy interesante, establece delitos genéricos, quizá faltaría por incorporar, hay muchos países ya en la comunidad andina lo han hecho, lo tiene argentina, lo tienen Colombia. Habrá que repensar la importancia de contar con una norma que no solamente establezca estos delitos genéricos, sino también coadyuva a la persecución de este tipo de ilícito, si observamos las normas que están contenidas dentro del convenio de cibercriminalidad de Budapest, hay muchas normas relacionadas con la cooperación internacional, y eso hace falta mucho dentro de la normativa para sancionar este tipo de ilícitos.

Entrevistado 3

En el gobierno tenemos un problema, actualmente no existe política criminal ni para lo que es fácil, mucho menos para lo que es difícil, a investigar de forma eficiente estos delitos el gobierno debe tener una planificación de expertos y política criminal para la investigación de delitos

informáticos porque eso no, no existe, como le digo no existe una planificación política criminal ni para delitos comunes, por esta razón tenemos incremento exagerado de la violencia, porque no hay una política criminal que la pueda parar. Entonces, esta política criminal debe ser planificada desde el punto de vista de la violencia, de la investigación y obviamente de la sanción posterior (inentendible), con la intervención de una persona que sepa de levantamiento de esta información digital, el hecho de resguardarla, darle los instrumentos para poder presentarlos con validez ante un tribunal penal, a veces existe el sistema, existe la máquina, existe la evidencia, el perito acostumbre a hacer una copia espejo, se pide un aparato para realizar esta copia espejo, no tenemos con que ¿Cómo le damos un disco duro para que haga una copia espejo? No hay forma, el perito de su bolsillo no lo va a comprar, porque está cobrando. Entonces, esta política criminal debería ir encaminado no solamente la planificación de los perseguimientos, sino también a una situación importante de recursos, porque en la actualidad, en la delincuencia común, pero es tremendamente alarmante el crecimiento de delitos que se cometen mediante sistemas informáticos.

Pero para eso, se necesita una planificación experta, primero, y segundo, en donde el estado, le preste atención a la seguridad cibernética de la gente.

Entrevistado 4

Si, esto está relacionado con lo anterior, considero que debe existir la pericia que lo hace el perito no es una de forma calificada y técnica. Es necesario actualizar los medios que nos encontramos en los cuales debe haber más esa capacitación de los peritos, que realizan este tipo de levantamiento de evidencias en el aspecto informático.

En la situación del delito, es una de las personas que están fijando y levantando y tratando de evidenciar las evidencias delictivas.

Entrevistado 5

Uno. Cambiar de gobierno. Segundo, no hay política criminal desde los estamentos públicos, porque la política criminal no es únicamente la persecución del delito, sino la prevención. Y desde la prevención vemos que en los delitos comunes y corrientes que se cometen, digamos online, o sea fuera del sistema informático, se incrementa porque no hay los procesos o requerimientos de seguridad extra. Peor aún si no se tiene articulado un organismo central de prevención, seguimiento, control, vigilancia de delitos informáticos. Eso implica que tanto Policía Nacional, cuanto el Ejército y Fuerzas Armadas en general deben estar articuladas con la Secretaría Nacional de Inteligencia para tener acceso a través de los sistemas informáticos y el seguimiento

respectivo. Hoy por hoy, lo máximo que se puede efectuar sin recurso económico es nada más el rastreo y seguimiento del teléfono celular. Pero no tenemos la capacidad por falta de justamente políticas públicas que nos vayan a permitir tener un mejor acceso, control y seguridad en la prevención, en el cumplimiento de sus delitos y por otros.

Entrevistado 6

Se debería por parte del Estado incorporar mayores seguridades para las entidades financieras como ya se viene haciendo en algunas entidades financieras y los usuarios realizar sus transferencias desde lugares seguros, pues hacerlo desde lugares públicos ha permitido ser perjudicados.

Entrevistado 7

En el conocimiento que tengo, Ecuador cuenta con normativa y procesos algo escasos. Se podría decir que incluso menos de lo requerido para hacer cara a las problemáticas. A mi criterio, sería muy positivo mejorar la política pública, mejorar la normativa respecto a delitos informáticos y protección de datos que, si bien existen, deben reafirmarse mucho más.

Adicional a esto es importante considerar la capacitación al personal y los recursos tecnológicos, los cuales requieren una gran inversión. En Ecuador contamos con el Ecucert, pero es insuficiente.

En la parte publica, en especial en el sector público, hace falta una inversión en materia de seguridad en términos de personal y equipamiento tecnológico requerido. Un caso muy palpable de esta falta son los relacionados con la filtración de datos, de información personal, los ataques informáticos recibidos por al ANT. Un tema critico es la falta de gestión de los organismos en torno a la información.

Entrevistado 8

Fortalecer la capacitación especializada en investigación y enjuiciamiento de delitos informáticos para los fiscales, jueces y otros operadores de justicia involucrados en estos casos, con esto me quiero referir más específicamente al Policía Judicial. Esto podría incluir el establecimiento de programas de capacitación y la provisión de recursos y herramientas especializadas.

Fomentar la colaboración entre los actores del sector público y privado en la prevención y el enjuiciamiento de delitos informáticos a través creación de alianzas público-privadas para intercambiar información y recursos en la lucha contra estos delitos.

Actualizar los reglamentos de las instituciones estatales que manejen datos sensibles para abordar adecuadamente los delitos informáticos, incluyendo protocolos claros de defensa informática.

Fortalecer la capacidad de investigación y análisis de la Unidad de Investigación de Delitos Informáticos y proporcionar recursos adicionales para investigar y procesar delitos informáticos.

Fomentar la concienciación y educación pública sobre los riesgos y las medidas de prevención de delitos informáticos, en particular para los grupos más vulnerables como los niños y los ancianos. Estas son solo algunas posibles medidas que podrían ser consideradas para fortalecer la política criminal del Gobierno central en la lucha contra los delitos informáticos.

Entrevistado 9

Para combatir y prevenir los delitos informáticos, es importante que el Gobierno central continúe fortaleciendo la capacidad de las autoridades encargadas de la investigación y persecución de estos delitos. Esto incluye la implementación de políticas y programas de capacitación y actualización de conocimientos y tecnologías. También se deben fortalecer las medidas de protección de datos personales y seguridad cibernética, y fomentar la cooperación internacional en la lucha contra la ciberdelincuencia

Entrevistado 10

A mi criterio personal, considero que la política criminal del Gobierno central debería fortalecer el enfoque preventivo y educativo en cuanto a la ciberseguridad, especialmente en el sector público y privado. Asimismo, se deberían establecer mecanismos para una mejor coordinación interinstitucional en la lucha contra los delitos informáticos, fomentar la especialización de los operadores de justicia en esta materia y mejorar la investigación y recolección de pruebas en casos de delitos informáticos. Además, se debería considerar la posibilidad de incluir nuevas figuras delictivas y actualizar las ya existentes en el Código Orgánico Integral Penal para estar acorde con la evolución de las tecnologías y los nuevos métodos utilizados por los delincuentes informáticos, total, para eso la constitución les da la iniciativa legislativa.

Comentario del autor

Evaluando la premisa de que la ley escrita no es un concepción autónoma, debiendo ser efectuada por el estado y la cohesión; y que la delincuencia es un fenómeno de carácter económico-social que no encuentra en la ley penal su solución, solo su contención y la reparación de los afectados, quedando la prevención entonces en las manos de la política pública, esta pregunta se

efectuó con propósito de que, a través de sus sugerencias, los entrevistados pudieran reflexionar sobre las políticas públicas que el gobierno haya emitido, y en consecuencia poder contratar los puntos a mejores, con las falencias indicadas en las tres anteriores preguntas.

Las respuestas se pronunciaron respecto de ciertas cuestiones modulares. La necesidad de una renovación en los reglamentos de actuación de agentes fiscales, peritos y otras dignidades que interactúen con medios probatorios digitales. La incorporación del Ecuador al Convenio de Ciberdelincuencia de Budapest. Y una incorporación de un plan nacional de prevención. Todas estas cuestiones son de gran valor, ya que en mi opinión son respuestas hacia las múltiples ramificaciones del problema que es la desatención del estado central sobre los asuntos de seguridad informática.

5. **El Estado ecuatoriano no se encuentra subscrito al Convenio de Ciberdelincuencia de Budapest ¿Estima usted que la no adhesión al convenio ha perjudicado el esfuerzo en la percusión de la justicia en el ámbito informático?**

Entrevistado 1

Bueno, en realidad el que Ecuador que este o no subscrito es algo secundario. Lo primero que habría que fortalecer es la política pública, que vaya encaminada a evitar a gran escala el cometimiento de los delitos informáticos. Recordemos que nosotros estamos subscritos a nivel internacional no exclusivamente a convenios que vayan en contra o que colaboren para evitar cometimiento de delitos informáticos, sino que es la falta de conocimiento de la ciudadanía, insistió, el conocimiento es fundamental sobre estos delitos informáticos que se encuentran en el Código Orgánico Integral Penal para luego si ver la importancia se subscribirse a este convenio de Budapest. Antes de esta pregunta es importante indicar que es el convenio, que figuras trae, si el Ecuador se subscribe, que debería hacer, pues recordemos no solo es la subscripción y ya. Al momento de subscribirnos hay que adoptar leyes de carácter vinculante, que ayuden a Ecuador a frenar estos delitos de ciberseguridad

Entrevistado 2:

Claro, evidentemente. Evidentemente la falta de adhesión de nuestro país a este convenio, yo creo que perjudica a la prosecución de este tipo de delitos. Una de las características, aparte de que los delitos informáticos afectan varios bienes jurídicos, es la transnacionalidad de los delitos informáticos, entonces, delito que se puede cometer estafas informáticas desde un servidor de China, pasar por Argentina y terminar perjudicando a personas en Ecuador, entonces existen

disposiciones dentro del Convenio de Cibercriminalidad relacionadas con la cooperación judicial, con la jurisdicción, qué jurisdicción se debe observar, se debe aplicar, etc. Yo creo que sí, ha perjudicado, sigue perjudicando y seguirá perjudicando hasta que no se pueda incorporar una norma, pero insisto, si podemos contar con una serie de normas, pero si no las aplica de la manera que corresponde, no existe la debida capacitación, la debida preparación, no existe una justicia especializada, vamos a recaer en lo mismo.

Ecuador acabo de reconocer una norma muy importante en materia internacional que es la Ley orgánica de protección de datos personales. Y ¿Por qué digo internacional? Porque es una norma, si bien es que tiene vigencia en nuestro país, pero que ha sido adaptada desde un marco internacional, que es el Reglamento General Europeo de Protección Datos Personales. Esa ley entro en vigor en mayo de 2021, si mal no recuerdo, entro en vigor, pero vamos a cumplir ya dos años en mayo de 2023 va a entrar en vigor del régimen de sanción, esa ley está vigente, pero vamos a ver cuántas instituciones en el ámbito público o privado han adaptado su normativa interna para garantizar la protección de datos personales de cualquier persona, etc. Entonces, incluso todavía no contamos con una autoridad de control que es la Superintendencia de Protección de Datos personales, estamos a 4 meses para que entre en vigencia el régimen de sanciones administrativas, pero contamos con una autoridad administrativa, si uno revisa por ejemplo, la incorporación de la autoridad de protección datos personales, como una autoridad administrativa con potestades de supervisión, control, investigación y de sanción, sancionar, si uno revisa la autoridad de protección de datos que en nuestro caso se trasladara a la Superintendencia de Protección de datos, es uno de los pilares esenciales para institucionalizar la vigencia de este derecho fundamental, pero hasta el momento no se lo ha hecho.

¿A qué quiero llegar con este ejemplo? Podemos tener todas las normas nacionales, internacionales, pero si no se hace nada para contar con esa justicia especializada en el ámbito de delitos informáticos, no se hace nada para contar con una autoridad, una justicia especializada, una justicia administrativa como es la función que deberá llevar a cabo la autoridad de protección de datos, no se hace nada para contar con esa justicia administrativa en la materia de protección de datos, justicia especializada, no vamos a llegar a ningún lado. Abundamos en normas, pero no hacemos nada para contar con mecanismos que sean eficaces para garantizar la protección de distintos derechos en el ámbito penal, delitos informáticos, en el ámbito constitucional, a través de la protección de datos personales, por ejemplo.

Entrevistado 3

Desde luego, porque usted conoce que de acuerdo con donde se ubique, determinan el procedimiento de la justicia. Entonces el hecho de pertenecer a ellos, y con ellos el estado está obligado a desafiar en los aspectos que subscribe, el hecho de no pertenecer y el momento realizar el levantamiento con desconocimiento de lo que se dice ahí pues, obviamente va a traernos prejuicio, para nosotros como ciudadanos ecuatorianos. Yo conozco casos de México y Colombia justamente tienen lo que usted me acaba de indicar, que por pertenecer a esta firma internacional tuvieron la oportunidad en ambos casos, en México en especial, en Colombia me parece que fue un tema de drogas que no lo tengo muy claro pero en México si, que se pudo localizar a un ciudadano que estaba en Inglaterra, me parece, realizando delitos contra la integridad sexual mediante el uso del internet en contra de menores, entones con este tratado, con la puesta en marca, el compromiso de las naciones que lo subscriben, lograron realizar el operativo en el momento que se efectuaba la infracción, entonces, al ciudadano lo sorprenden en el domicilio con la computadora, manteniendo ese momento contacto con presuntamente la menor, pero que era un agente, que estaba haciéndose pasar por ella.

Le comento, nos dieron un curso de ciberdelito hace aproximadamente unos seis o siete años que nos comentaron ese caso, y nos pareció muy interesante, y nos extrañaba la falta de presencia del ecuador en estas, en las suscriciones estas.

Entrevistado 4

Claro. Bueno, yo pienso que en realidad el Estado al ser suscriptor, o a lo mejor que acabe siendo legatario después, del sentido de la adhesión y aprobación en el sistema ecuatoriano, este tipo de delitos a través de la informática, obvio, es transnacional y de hecho se están cometiendo. No solo considero solamente la adhesión, sino también la cooperación internacional e institucional para poder ver una forma integral de los Estados y combatir la delincuencia que se da a través de esos medios telemáticos.

Entrevistado 5

Sí, porque el convenio, como te decía en principio, no únicamente es de determinación de delito, sino también en la parte procesal y en la parte procesal. Es la coordinación y cooperación interinstitucional o intergubernamental. Y si no hay dos partes de ese convenio, evidentemente no te nutres de toda la información que, por ejemplo, la Policía europea en delitos informáticos ya tiene como horas de vuelo o experiencia. Asimismo, la Policía americana, el FBI, CIA y todos los

estamentos de vigilancia y control tienen como experiencia desde la casuística que ellos ya han tenido desarrollada en sus países. Y evidentemente que sí. Es una debilidad que el Ecuador no haya suscrito este convenio, tanto más que en Naciones Unidas está realizando otro convenio que supla al de Budapest y que englobe ya a la mayor cantidad de países a nivel global.

Entrevistado 6

Indudablemente tratándose de este tipo de delincuencia es válida toda acción encaminada a la cooperación y asistencia para evitar ser sujetos de delitos informáticos.

Entrevistado 7

Si bien es cierto, la adhesión sería ventajosa1, debemos analizar los compromisos que vienen con él. Un punto del convenio establece el intercambio de datos, pero para llegar a ese punto el estado necesita tener antes una madurez normativa y tecnológica para proteger los datos de los ciudadanos. Entonces, entendemos que la adhesión sería sumamente beneficioso, pero Ecuador debe primero contar con ciertos recursos para plantearse entrar ahí, de lo contrario podría perjudicarnos, al no cumplir con nuestros compromisos.

No creo que nos haya perjudicado el no estar integrados, ya que existen elementos procesales que nos permiten dar con los mismos resultados, quizá algo más demorados, pero concluyendo.

Entrevistado 8

La falta de adhesión del Estado ecuatoriano al Convenio de Ciberdelincuencia de Budapest puede haber tenido un impacto negativo en los esfuerzos de persecución de la justicia en el ámbito informático. El Convenio de Budapest es el primer tratado internacional que aborda los delitos informáticos y tiene como objetivo establecer medidas comunes para prevenir y combatir la ciberdelincuencia a nivel internacional. La adhesión al convenio proporciona una plataforma para la cooperación y la coordinación internacional en la lucha contra la ciberdelincuencia, incluyendo la armonización de leyes, la asistencia judicial mutua y la promoción de la capacidad y la capacitación en ciberseguridad.

Al no ser parte del Convenio de Ciberdelincuencia de Budapest, el Estado ecuatoriano puede encontrarse limitado en su capacidad para cooperar internacionalmente en la lucha contra los delitos informáticos y puede estar en desventaja en la adopción de medidas internacionales para combatir esta problemática. Además, la falta de armonización internacional de leyes y medidas de protección en el ámbito de los delitos informáticos podría dificultar la persecución de delitos

cometidos por delincuentes que se encuentran en otros países.

En resumen, la no adhesión del Estado ecuatoriano al Convenio de Ciberdelincuencia de Budapest puede haber tenido un impacto negativo en los esfuerzos de persecución de la justicia en el ámbito informático, especialmente en términos de cooperación y coordinación internacional. Ser parte de este convenio podría ser una medida importante para fortalecer la capacidad de Ecuador para combatir los delitos informáticos y proteger a sus ciudadanos en el mundo digital.

Entrevistado 9

La no adhesión del Estado ecuatoriano al Convenio de Ciberdelincuencia de Budapest podría considerarse un obstáculo para la lucha contra la ciberdelincuencia a nivel internacional, ya que este convenio establece un marco de cooperación para la investigación y persecución de delitos informáticos entre los países que lo han suscrito. Al no ser parte del convenio, Ecuador podría tener dificultades para acceder a información y recursos necesarios para la investigación de delitos informáticos que involucren a otros países que sí sean parte del convenio. Además, el no estar adherido al convenio podría generar una percepción de falta de compromiso del Estado en la lucha contra la ciberdelincuencia a nivel internacional.

Entrevistado 10

Considero que la no adhesión del Estado ecuatoriano al Convenio de Ciberdelincuencia de Budapest ha afectado a la cooperación y el intercambio de información internacional en la lucha contra la ciberdelincuencia. Este convenio es un instrumento importante para la armonización de la legislación penal informática a nivel internacional y para la promoción de la cooperación entre los Estados en la investigación y persecución de delitos informáticos. Además, su adhesión puede mejorar la percepción de confianza en el país para la inversión extranjera y el desarrollo de tecnologías de la información.

Comentario del autor

La pregunta quinta fue formulada en concordancia con el objetivo específico de determinar si el Convenio de Budapest sirve como un marco procedimental y jurídico efectivo el cual la legislación ecuatoriana se beneficiaria de acogerse como marco referencial. Los entrevistados fueron cuestionados sobre su impresión sobre la falta de adhesión de la República del Ecuador al Convenio de Cibercriminalidad. Aunque los entrevistados fueran profesionales del derecho relacionados con la legislación informática, previamente se les dio una breve introducción e indicaciones de este, para contextualizar la pregunta.

Las respuestas emitidas por los entrevistados fueron unánimes en favor de la adhesión, aunque con sus respectivas reservas y adhesiones. En términos generales se estimó que la cooperación internacional y el marco jurídico que ofrece esta convención son de necesidad importante para la república, entendiendo que si bien la legislación informática penal existe en el ecuador, cualquier falla de la ley podría suplirse sobre los términos de esta legislación y además los mecanismos de cooperación establecidos dentro de ellos, que atendería de manera eficaz el problema de la transaccionalidad que caracteriza a este tipo de delitos y otros relacionados de paso, como el crimen organizado transnacionalidad involucrado. Personalmente resalto los argumentos expuestos por el segundo entrevistado, que se expresa adecuadamente sobre el problema de la transaccionalidad, sobre la cual se pronuncia como evidentemente problemática. Al mismo tiempo que expone que contrasta su posición y explica que el Convenio no es una fórmula mágica, exponiendo las necesidades de mecanismos especializados que puedan sujetar las obligaciones y herramientas que presta este convenio, refiriéndose especialmente sobre la justicia especializada, y la aun hoy no materializada Superintendencia de Datos. Esta posición es de gran valor para este trabajo, y como subscritor del mismo expreso mi concordancia con la misma en razón que expone un contraste de valor importante a tener en cuenta respecto de lo que se pueda exponer como ventajas del convenio, ya que se debe esclarecer que el país está especialmente necesitado de infraestructura especializada para combatir a la delincuencia informática, punto de valoración especial cuando se exponga respecto de las conclusiones y lineamientos derivados del objetivo específico segundo.

6. **A su experiencia en el campo sobre los delitos informáticos ¿Qué lineamientos estima necesarios en implementar dentro del ámbito jurídico ecuatoriano para poder solventar los mencionados problemas?**

Entrevistado 1

Personalmente, encuentro problemática la realidad del manejo de las pruebas y la actuación de los fiscales, a mi opinión, tendríamos que partir haciendo reformas y mejoras en la estructura interna de la Fiscalía General del Estado, ya que si bien no creo que el Código Penal sea perfecto, es cierto que tiene figuras con las que se puede trabajar, pero si el personal encargado de hacer ejercicio de la misma se encuentra tan infra capacitado para la labor y tan precarios en recursos materiales, poco efecto tendrá cualquier incorporación de nuevos tipos penales o adhesiones a tratados internacionales.

Entrevistado 2

En primer lugar, creo que hay que reiterar en lo que hemos dicho, capacitación de las personas vinculadas con el tratamiento de evidencia electrónica, evidencia digital, eso vincula fiscalía, vincula a jueces de garantías penales, etc. El saber determinar la importancia de las reglas que tienen que ver con los principios que se aplican a la evidencia electrónica. Los mismos principios que se aplican a la evidencia general, se aplican también por ende a la evidencia electrónica.

Y una regla muy interesante en el Código Orgánico Integral Penal, no recuero ahora mismo la disposición, por ejemplo, se puede hacer un reconocimiento de un lugar de los hechos en territorio digital, entonces cuando revisa la norma procesal en el Código Orgánico Integral Penal dice reconocimiento del lugar de los hechos, un accidente de tránsito se realiza un reconcomiendo del lugar de los hechos, el lugar donde se cometió, donde existió un accidente; reconocimiento del lugar de los hechos en territorio digital, es decir, el reconocimiento de los medios que posibilitaron o permitieron cometer una infracción informática.

Entonces, saber entender, discernir que tipo de evidencias, como proceder, cual es la actividad que deben cumplir los forenses digitales, etc. Entonces todo ese escenario, nos lleva a la necesidad de contar con mayor preparación. Luego, si evidentemente, el sistema no cambia, es evidente esta característica, o esta necesidad; si el sistema cambia, o debería cambiar, deberíamos contar con una justicia especializada, es decir, debería haber una fiscalía como se promovió ahora, se está intentando promover en materia penal a través de esta última resolución de la Fiscalía General del Estado, es decir, contar con una fiscalía especializada para la investigación o persecución de delitos informáticos, deberían existir jueces especializados en delitos informáticos, deben existir garantías específicas para las víctimas, y todo esto también implica mecanismos que permitan a la gente conocer, consciencia, no solamente es el ámbito de la prevención, sino también del ámbito de decirle a la gente, a la ciudadanía, usted cuenta con estas herramientas, usted cuenta con estas posibilidades de denunciar ante determinada autoridad, etc.

Yo creo que las políticas públicas juegan un papel importante, de hecho, es uno de los principios para la aplicación de los derechos, cuando revisa el 11. 8 de la Constitución, dice los derechos se desarrollarán de manera progresiva a través de las normas, políticas públicas y la jurisprudencia. Bien, citaba al inicio la política para una internet segura de niños, niñas y adolescentes que fue promovida por el Consejo Nacional para la igualdad Intergeneracional,

llevamos ya casi dos años, pero hay que ver si se está implementando de manera consciencia, en las instituciones educativas, en las empresas, etc. Entonces, sí, es importante pero la forma en que se promueve, la forma en que se ponen en práctica, ahí hay que repensar la forma en que se lo hace.

El problema de los derechos en sentido general, o el problema del derecho, no está en contar con normas, códigos etc. Sino en la forma en la que se los hace vigente en la práctica, ese es el verdadero problema de los derechos y garantías, la forma en que se pueda promover y hacer efectivo esos derechos, sobre todo en materia penal, hablando de delitos informáticos.

Entrevistado 3

Puede ser principalmente el enfoque concreto de conductas que sean, si bien no tipificadas o descritas en el tipo penal de forma simple, pero que se mantengan actualizadas conforme avance, es decir que se actualice de forma constante, porque este es un tema que no se puede quedar aquí, como es el robo, la violación, como es el homicidio. Se transforman constantemente, y es importante, y sería ideal y la comisión de legislación, la comisión de legislación de la asamblea sea la que estén al día en esto, pero lamentablemente se ocupan en otras cosas, entonces no se ocupan en lo que verdad sucede, y así mismo el hecho de darnos las facilidades y que se describa de forma previa que acciones tenemos permitidas como agentes fiscales, en el caso nuestro, para poder preservar esta evidencia, en el caso nuestro, para poder preservar esta evidencia, hasta donde nosotros podemos ingresar a un sistema, por ejemplo, un sistema público pero para realizar una investigación, entonces todas estas cosas nos faltan, todavía hay bastantes vacíos procesales, tanto como objetivos de la investigación.

Entrevistado 4

Sí, claro. Bueno, en la situación que actualmente vivimos, que se ha tenido en esta Fiscalía de investigación, es que los peritos, a través del sistema de criminalística, han establecido que no tienen, por ejemplo, programas estandarizados de los lineamientos que incluso de afuera de extranjero manejan técnicas informáticas más de data avanzada y la cual Ecuador o Latinoamérica mismo no tiene este sistema informático. Considero que en realidad el problema está ahí, en manejar un cuerpo de peritos que estén actualizados con ese sistema, con este programa, con estas plataformas virtuales, que a lo mejor es de fácil acceso, pero de muy difícil identificar de dónde son este lo que se produce la información.

Entrevistado 5

En el tema de tipos penales primero va la sociedad adelante y conforme la sociedad va

realizando cierto tipo de conductas que son socialmente rechazadas, en su momento, se reforma la ley. Entonces, en ese sentido sí habría que revisar el contenido normativo del Código Penal a efectos de que se puedan incorporar nuevos tipos penales desde la perspectiva del juzgamiento y tipificación de esas conductas.

Y para eso, evidentemente, si es que no se suscribe el tratado, se podría reflejar como espejo que delitos ahí se contienen y se podría reformar el Código. La no suscripción del tratado implica básicamente no acuerdos de cooperación, más no el no poder reformar nuestra legislación. Y en la parte procesal se debería establecer un procedimiento especial para el tratamiento de estos delitos informáticos, tomando como sustento base la demora en la obtención de información. Entonces, si en un delito de robo, hurto, violación o femicidio, por último, se tiene físicamente la evidencia, es más fácil acceder a ella y es más fácil tener esa información, ADN, examen médico legal, etcétera. Pero en el tema informático esos tiempos se relativizan porque no es lo mismo ir a un lugar in situ, en físico y hacer el reconocimiento del lugar de los hechos, que extraer toda la información de una red informática que tiene diferentes IPS a nivel global y que finalmente vienes a hacer un rastro para saber de dónde salió esa información, ese contenido, ese link para que puedas acceder y modificar tus cuentas, etcétera.

Entrevistado 6

En el caso de delitos informáticos estimo se debería juzgar incluso en ausencia del procesado, sin que limite la posibilidad de que el Estado repare el daño causado a la víctima para luego ejercer el derecho de repetición contra los responsables.

Entrevistado 7

Yo considero que se debe tener un proceso claramente establecido acerca de cómo se debe actuar frente a delitos informáticos. Es decir, una normativa expresa que enumere claramente los pasos a seguir. En chile se tiene basto expendio de documentos para cada caso y situación, por ejemplo, si la información está en equipos se detalla perfectamente el proceso a seguir. Desde la recolección, el análisis y la entrega del informe. Sumado a esto, no basta solo con la norma, también debe haber personas que supervisen que dicha norma se está cumpliendo. En la actualidad existe normativa, que queda casi al criterio de las personas el sí aplicarla o no aplicarla.

Sería importante además el optimizar el sistema pericial, algo infravalorado. En mi especialidad puede percibir hasta 10 salarios básicos como remuneración, teniendo casos donde se deben revisar hasta 20 o 30 equipos, y por tanto la paga no cubre ni el 15 o el 20% de lo que en

realidad vale ese servicio. Aquí hablaríamos de un factor motivacional para el trabajador.

Entrevistado 8

Sería bueno actualizar y mejorar la legislación penal y procesal para que sea más efectiva y se adapte a la rápida evolución de la tecnología.

Promover la cooperación y coordinación internacional en la lucha contra la ciberdelincuencia a través de acuerdos y convenios internacionales, como el Convenio de Ciberdelincuencia de Budapest debería ser una prioridad dentro del contexto actual

Fomentar la capacitación y especialización de los jueces, fiscales y abogados en temas relacionados con los delitos informáticos para que puedan enfrentar eficazmente los casos relacionados con la ciberdelincuencia.

Desarrollar medidas de protección y seguridad para prevenir la comisión de delitos informáticos, como la promoción de políticas y estrategias de seguridad cibernética y el fortalecimiento de las capacidades tecnológicas de las instituciones.

Entrevistado 9

Algunos puntos a tomar a consideración sería la necesidad de actualización y mejora constante de las leyes y normativas existentes para adecuarlas a la realidad cambiante de la tecnología y los delitos informáticos.

Fortalecer la capacitación y actualización de conocimientos y tecnologías de las autoridades encargadas de la investigación y persecución de delitos informáticos, en conjunto con la mejora de la coordinación y cooperación entre las distintas autoridades encargadas de la investigación y persecución de delitos informáticos.

Sumado a esto es fundamental hacer un esfuerzo en el fortalecimiento de la protección de datos personales y la seguridad cibernética y la promoción de la cooperación internacional en la lucha contra la ciberdelincuencia.

Entrevistado 10

Actualizar y mejorar la legislación penal en materia de delitos informáticos, para que sea más específica, clara y efectiva en la persecución de este tipo de delitos.

Fomentar la capacitación y formación de jueces, fiscales, policías y otros actores del sistema judicial, en temas relacionados con la tecnología y la informática, para que puedan entender y manejar adecuadamente las pruebas y evidencias digitales en los procesos judiciales.

Implementar políticas y programas de concientización y prevención en temas de seguridad

informática y protección de datos personales, dirigidos a la sociedad en general y especialmente a los sectores más vulnerables, como los niños y jóvenes.

Asegurar la protección de los derechos fundamentales de los ciudadanos, incluso en el ámbito digital, garantizando la privacidad, la libertad de expresión y la no discriminación en línea.

Comentario del autor

Esta última pregunta, al ser la culminación de los puntos explorados alrededor de toda la entrevista, y al ser también culminación de puntos explorados previamente en la doctrina y marco teórico de este trabajo de integración curricular; busco explorar en la experiencia de quienes conviven con los efectos de la ley, medios indicativos respecto a cómo enmendar los problemas de la aplicación efectiva de la norma jurídica. Todo esto se consiguió a través de solicitar a los entrevistados que contribuyeran con su perspectiva respecto de soluciones, no en un intento de que estos suplantaran la responsabilidad de este trabajo de investigación, sino en el lograr conseguir una perspectiva más concisa sobre los problemas más inmediatos, ya que donde una trabajo de investigación que se enfoca en la norma, va a tener soluciones tan generales como su ámbito de aplicación, una opinión de quien vive bajo los efectos y al ejercicio de los procesos que esta misma norma dispone, tiene una opinión más detallista respecto de las alteraciones necesarias para un mejor funcionamiento.

Los puntos de vista ofrecidos por los entrevistados muestran en general un acuerdo general en la necesidad de una reforma sobre el aparato fiscal y perital, especialmente enfocado en sus prácticas y la capacidad operativa que estos manejan; teniendo gran relevancia y preocupación por parte de los entrevistados el manejo de los medios probatorios y la cadena de custodia cuando de medios probatorios digitales trata.

6.1.3 Estudio de Casos

6.1.3.1 Caso de estudio

1. Datos Referenciales

No. Procesos: 17282-2019-01265

Acción: Ataque a la Integridad de Sistemas Informáticos. Numeral 1. Reformulado a Acceso no consentido a Sistema Informático.

Ofendido: Corporación Nacional de Telecomunicaciones EP.

Acusado: O. M. M. B

Juzgado: Tribunal de Garantías Penales con Sede en la Parroquia Iñaquito del Distrito

Metropolitano de Quito, Provincia de Pichincha.

Fecha de ingreso: 16/07/2021

2. Antecedentes

O. M. M. B es un ciudadano sueco que fue detenido el 11 de abril de 2019, en el Aeropuerto de Tababela Quito, ante una denuncia realizada anónimamente al 1800-Delito. Posterior a esto, el día siguiente, el 12 de abril de 2019, tuvo lugar la audiencia de formulación de cargos, donde le fue imputado el delito de Ataque a la integridad de Sistemas Informáticos, en lo respectivo de su numeral primero, contenidos en el Artículo 232 del Código Orgánico Integral Penal.

Ese mismo día, en la madrugada, su vivienda fue allanada por personal de la Policía Nacional. En la misma audiencia de formulación se le dictaron las medidas cautelares de prisión preventiva y retención de cuentas. Cabe menciona que, en el acta de formulación de cargos, fiscalía no precisa ni conoce respecto de que sistema fue atacado.

El 15 de abril de 2019, O. M. M. B impuso a través de su defensa una apelación respecto de la prisión preventiva dictada en su contra, misma que paso a la Sala de lo Penal Militar de la Corte Provincial de Pichincha. El 25 de abril de 2019 se autorizó respecto de la extracción de información de los dispositivos incautados en el allanamiento de la morada de O. M. M. B. El 2 de mayo de 2019, la Sala de lo Penal de la Corte Provincial rechazo la apelación. 29 de mayo, se niega la fianza en audiencia.

Cabe señalar que O. M. M. B antes de la imputación de cargos tuvo un contexto geopolítico de peso, ya que este era cercano al hacker internacional Julián Assange, siendo señalado por parte de inteligencia estadounidense como un hacker que operaba desde aquí.

El 22 de agosto de 2019, CNT realizo acusación particular del Estado llevo la teoría del caso de que el O. M. M. B había ingresado sin autorización, con ayuda de un segundo, a la IP LAN de CNT sin autorizaciones correspondientes, afectando así la información y la seguridad de los archivos.

El 29 de agosto de 2019, la Fiscalía solicito la reformulación de cargos, cambiando la acusación al delito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones, estipulado en el artículo 234 del Código Orgánico Integral Penal. Como medios probatorios presentados por fiscalía sobre el hecho se adjuntaron fotos recogidas del teléfono personal del acusado, en el cual se mostraba dentro del Sitio Web de CNT.

3. Resolución

La resolución del tribunal se dictó con fecha 31 de enero del 2023. Con voto unánime, el Tribunal de Garantías Penales de Pichincha dicta que valorando que las pruebas presentadas no demuestran en ningún momento la vulneración del sistema de seguridad de CNT o cualquier sistema de protección. Y al no configurarse como tal una infracción, el tribunal se expresó en sentencia ratificando la inocencia de O. M. M. B.

Comentario personal del autor

Este caso es sumamente significativo para este trabajo, ya que es una expresión de lo ajeno que son los conceptos informáticos para la justicia, haciendo hincapié en la fiscalía general del Estado, la ambigüedad de los tipos establecidos en el Código Orgánico Integral Penal y la incompetencia del personal fiscal y policial respecto a la naturaleza y funcionamiento de los medios probatorios informáticos. Para comprender la relevancia de esta sentencia se debe partir del entendimiento del carácter político del proceso.

Como se explicó O. M. M. B. fue un sujeto de relevancia política por su relación con Julián Assange. El proceso, criticado por sus fallas en el debido proceso, muestra problemas serios en la persecución de la justicia por parte de la Fiscalía, misma que al momento de detener al acusado, no sabe pronunciarse sobre qué sistema fue supuestamente atacado por el mismo; no es sino hasta que existe una acusación particular de la Corporación Nacional de Telecomunicaciones, que conseguimos configurar uno de los elementos constitutivos más importantes del delito. Sin embargo, no solo se tuvo que reformular los cargos por no poder acoplar adecuadamente el delito al 232, sino que en la formulación y fundamentación sobre el 224, se tomaron como evidencias del acceso no autorizado, alertas de solicitudes de acceso negadas, a través del protocolo http, que se considera inseguro, que más bien, probando de este modo, y sin entender el significado de estas alertas, que el acusado no ingreso en ningún momento a la IP LAN. Únicamente se ingresó al sitio Web de CNT, nunca a su sistema.

Las falencias en el rol de la Fiscalía tienen dos vertientes, la primera, un uso abusivo del tipo del 232, que ha sido acusado de premeditado y político por parte de la opinión pública; y la segunda, un completo desentendimiento de los aspectos técnicos de la tipología a explorar, donde no solo la fiscalía nunca logro determinar qué sistema había sido atacado en su primera acusación, además pretendió probar la culpabilidad del acusado, a través de una prueba que no solo era inadecuada, siendo una foto de un sitio web encontrada en el teléfono incautado, sino que aparte probaba la tesis contraria a la sostenida por fiscalía, la cual actuó claramente sin conocimiento al

respecto del significado que tenían estas acciones delictivas mostradas en la fotografía. Estas falencias exponen y comprueban la carencia de capacitación técnica, sobre la cual se referían anteriormente los especialistas en derecho entrevistados.

Como se podía esperar de la situación, la sentencia del tribunal fue unánime en favor del acusado, quien fue probado libre de toda responsabilidad, y con puerta abierta a acciones legales consecuentes, puesto que además de que la acción emprendida por la fiscalía podría ser calificada de temeraria, hay señales y acusaciones de múltiples violaciones del debido proceso dentro de la causa.

6.2 Datos estadísticos

6.2.1 Numero de Noticias de Delitos Informáticos consumados en el Sistema Integrado de Actuaciones Fiscales

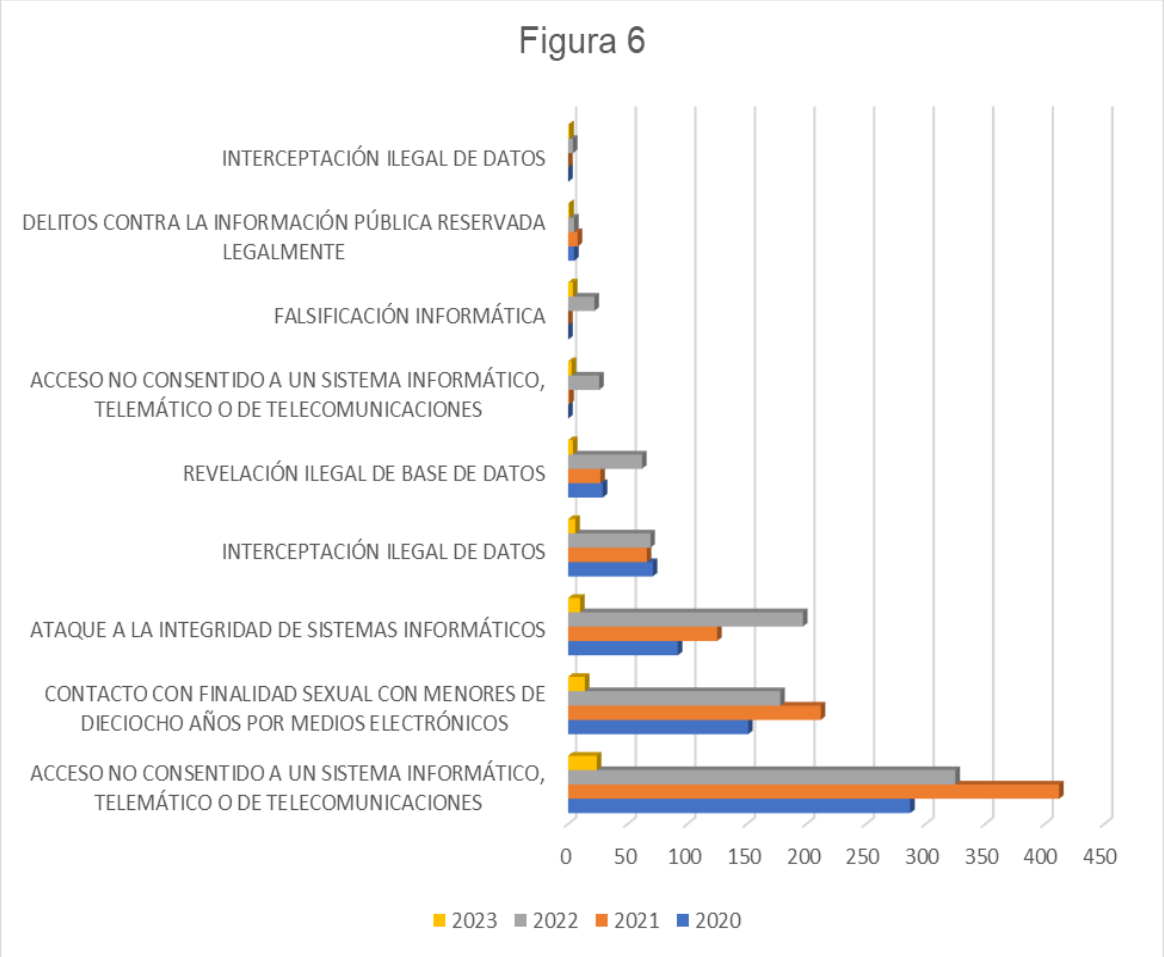

Ilustración 6. Número de Delitos Informáticos consumados en el Sistema Integrado de Actuaciones Fiscales.

Fuente: Fiscalía General del Estado

Autor: Joe Sebastián Contento Martínez

El presente cuadro se ha configurado con datos proveídos por parte de FGE, respecto de las noticias de delitos informáticos consumados que se notificaron en sistema de actuaciones. Los datos se detallan desde el año 2020, año solicitado debido al inicio de la pandemia y de la expansión de los trabajos remotos en consecuencias, hasta el presente año. En el grafico se puede observar una evolución histórica que se puede evaluar en base a sucesos relevantes en los últimos años. En 2020, podemos observar que existe una base fuerte de actividad delictiva en estos ámbitos, siendo el año donde la comisión fue moderada en delitos como el acceso no consentido y la revelación de bases de datos, sumado a una cantidad significativa en los ataques a la integridad de los sistemas. Esto tiene una explicación simple en el fenómeno de la Pandemia, la falta de preparación de los trabajadores que se unieron al teletrabajo, la legislación atrasada y los problemas operativos de las instituciones de justicia derivados del encierro repentino. De ahí en adelante, observamos un 2021 que repunta una vez consolidada la realidad informática, lo cual coincide con los incidentes del Banco de Pichincha, las plataformas digitales de captación de dinero y la consecuente promulgación de las reformas al Código Orgánico Integral Penal y la Ley Orgánica de Protección de Datos Personales, indicando que ese fue un año pendular, un punto de inflexión que se hace evidente al incrementar volátilmente los delitos con relación al año anterior. Por último, el año 2022 es el año donde se consolidan ciertos efectos de los cambios legislativos, pudiendo observar una retracción en los delitos acceso no consentido y grooming, aunque con un aumento en delitos que antes no eran tan relevantes en números, hechos que se explican en el traslado de los esfuerzos de los sujetos criminales fuera de los delitos más cifrados puesto que estos fueron también los más regulados, y hacia otras actividades que si bien han sido regulados, no tienen tanta atención debido a sus anteriores cifras sin peso.

Independientemente de los cambios respecto ciertos delitos, el grafico concuerda con una realidad que tanto en la opinión de los profesionales, como en las notas de prensa ya se ha mencionado, que es el incremento sostenido de los delitos informáticos a pesar de su retraimiento en 2022.

7. Discusión

7.1 Verificación de los objetivos

Los objetivos que se manejan en este trabajo son un Objetivo general y dos específicos, los

cuales se detallaran más adelante

7.1.1 Objetivo General:

- **"Realizar un estudio jurídico y de derecho comparado respeto del derecho informático."**

El objetivo general planteaba la obligación de realizar dos estudios, comprendidos por un estudio jurídico y un estudio de derecho comparado.

El primero de estos objetivos, el jurídico se realizó dentro del marco jurídico de trabajo. Mas específicamente se abarcaron desde el puto 1.8 al 1.16. En estos se analizó, con ayuda de punto de vista doctrinarios, los conceptos jurídicos involucrados y derivados del delito informático. Así mismo, posteriormente dentro del estudio de derecho comparado, se ofreció un análisis al detalle respecto de los articulados vigentes dentro del ordenamiento penal vigente.

El segundo objetivo se desarrolló en el numeral 2. Se realizo un análisis primerizo de los tipos expresados al momento, sobre derecho penal informático en el Código Orgánico Integral Penal. Teniendo la perspectiva completa respecto de estos, se procedió a exponer las legislaciones extranjeras. Se selecciono legislaciones relacionados con el derecho penal informático vigentes en los estados del Reino de España, la República de Chile, la República Federal Argentina y la República de Colombia, todas participes del Convenio de Budapest. Estas mismas se sometieron al contraste respecto del ordenamiento jurídico, teniendo especial relevancia la legislación española, que, por su contexto de primer mundo, su exitoso acoplamiento a la realidad informática, y su pertenencia al Consejo de Europa que fue quien redacto el convenio antes mencionado, muestra varios tipos penales que se encuentran al día con las necesidades de la realidad informática moderna. No obstante, el Ecuador, cabe mencionar, no se ha quedado atrás en términos de legislación penal, contando el Código Orgánico Integral Penal con un repertorio de normativo que en el papel es bastante competente, pero que pierde gran parte de su valor en su aplicación y socialización, sumado a la desactualización de ciertas figuras que si bien existen, como la estafa, no cuentan con un apartado particular o inciso que trate sobre su desarrollo en medios informáticos, ignorando la nueva realidad, entre otros artículos que requieren una actualización.

7.1.2 Objetivos Específicos:

- **"Determinar si los tipos establecidos en la actual legislación penal respecto al fenómeno de la criminalidad electrónica son efectivos para la persecución del mismo".**

El presente objetivo se comprobó en las actuaciones del análisis jurídico, las encuestas, las

entrevistas y la legislación comprada. Es decir, tuvo un uso extensivo del uso del método analítico, científico y comparativo para su consecución.

El análisis jurídico de los delitos informáticos contenidos en el Código Orgánico Integral Penal sirvió para a través de una disección de sus elementos comprender los propósitos de esta, y concluir respecto de imprecisiones, ambigüedades y consecuencias de estas tipologías. Por supuesto, la ley no existe por sí misma en una burbuja, y su impacto real se deriva de su aplicación a través del aparato estatal-social, no obstante, el primer acercamiento permitió aseverar aciertos y errores de la legislación que fueron valorados al momento de explorar las siguientes actuaciones.

Las encuestas dirigidas a profesionales del derecho incorporaron este objetivo específico dentro de su pregunta primera "¿Estima usted que la legislación penal vigente en términos informáticos es suficiente y ofrece los mecanismos procesales y tipos adecuados para la persecución del fenómeno de la ciberdelincuencia?"; y segunda "En base sobre su experiencia en el campo ¿estima que en ordenamiento jurídico actual es practico y procesalmente viable perseguir acciones informáticas que se desarrollaron en las redes?" que buscaban evaluar respecto del efecto real y practico que tenían las tipologías exploradas y analizadas previamente, mismas que concluyeron problemas en la aplicación de las tipologías establecidas por cuestiones propias, como al ambigüedad establecida en los términos de la tipificación; y problemas externos derivados de las falencias en actuación del recurso humano del sistema de Justicia como los peritos y agentes fiscales.

Idénticos propósitos, y resultados, tuvieron las preguntas primeras "¿Qué opinión le merece usted el estado actual de la legislación penal informática tipifica dentro del Código Orgánico Integral Penal?" y segunda "¿Encuentra que los mecanismos de persecución formalmente configurados en el ordenamiento actual son procesalmente eficientes y eficaces?". Siendo la diferencia, que las preguntas de la entrevista buscaban un desarrollo más extenso y contrastado respecto del estado de la legislación informática, en contemplación que quienes respondieron eran personas familiarizadas fuertemente respecto a la tipografía y su funcionamiento. Lógicamente, fue necesario el método analítico y científico a profundidad en estos apartados, respecto del procesamiento de la información recolectado, y su correcta obtención respectivamente.

Por último, se hizo uso extensivo del método comparativo en la legislación comparada, al establecer fortalezas, inobservancias, imprecisiones, vacíos y ambigüedades en el Código Orgánico Integral Penal actual al someterlo a estudio comparativo con las legislaciones de España, Código

Penal Español; Chile, Ley 19233, Argentina; Código Penal de la Nación; y Colombia, Ley 1273.

En este estudio resalto por sobre todo la legislación de la República de Colombia por su vigencia a pesar del tiempo, siendo aprobada en el año 2009, gracias su uso correcto del lenguaje técnico, la identificación de los elementos que la acción penal buscaba afectar y el evitar usar términos cuyo uso técnico pueda limitar u arbolecer la vigencia de la ley con el pasar del tiempo y el desarrollo de la tecnología.

- **"Determinar si el Convenio de Budapest sobre ciberdelincuencia sirve como un marco procedimental y jurídico efectivo el cual la legislación ecuatoriana se beneficiaria de acogerse como marco referencial".**

Este objetivo se buscó completar a través de tres vertientes. La primera, la incorporación de la pregunta tercera en la encuesta "¿Aprecia conveniente a los intereses del Ecuador el adoptar marcos internacionales como mecanismo para modernizar su legislación en cibercriminalidad y delitos informáticos?"; y la quinta pregunta de la entrevista "¿Aprecia conveniente a los intereses del Ecuador el adoptar marcos internacionales como mecanismo para modernizar su legislación en cibercriminalidad y delitos informáticos?" que buscaban exponer la percepción de quienes hacen ejercicio de los términos del Código Orgánico Integral Penal, y hacer análisis para poder concluir sobre los beneficios de este código y la percepción de necesidad de los profesionales del derecho, que se concluyó absoluta en su favor.

Como segunda vertiente, se hizo un análisis de los términos del convenio con un fin primerizo de conceptualizar los delitos informáticos a través de una nomenclatura globalmente aceptada, y análisis los términos de este código, con el fin de evaluar respecto de su valor como marco jurídico, haciendo uso del método analítico y comparativo, ya que se logró contrastar respecto de concepciones doctrinarias sobre los términos recogidos.

La tercera vertiente fue una de contraste indirecto, ya que las legislaciones a comparar con el Código Orgánico Integral Penal son todas productos de países miembros del Convenio de Budapest que ya se han acoplado. Esto tuvo el propósito de ver las diferencias entre el estado actual de la tipología penal y lo que esta podía llegar a ser con la influencia de esta convención, reflejado en las tipologías de las legislaciones a comparar. Se hizo uso extensivo del método analítico, inductivo y deductivo para este propósito.

- "**Determinar si la política pública por parte del gobierno nacional ha tenido o no efecto para poder combatir la ciberdelincuencia durante los últimos dos términos**

presidenciales".

A causa de la poca visibilidad de estas políticas, lo cual ya es una prueba de la desatención y carencia de impulso del ejecutivo, se buscó hacer una comprobación de este objetivo a través del destinatario de las políticas públicas, especialmente las campañas de concientización, por lo cual se incluyeron en la encuesta la pregunta "¿Considera que el Gobierno central ha aplicado una política pública criminal que haya aplacado o disminuido los delitos informáticos y la cibercriminalidad?" y la pregunta cuarta de las entrevistas "A su criterio personal ¿Que le faltaría implementar o modificar a la política criminal del Gobierno central para combatir y prevenir los delitos informáticos?". La primera para evaluar respecto del si los esfuerzos políticos del gobierno estaban teniendo algún efecto preventivo o disuasivo, y el segundo con el fin de evaluar mejoras, y un aislamiento más hermético respecto a que elementos específicos fallan en las políticas públicas. Los resultados de estos esfuerzos resultaron inesperados, ya que antes que pronunciarse sobre las políticas públicas, la población se expresó respecto de una evidente inexistencia, siendo imposible entonces exponer una evaluación de estas más allá de la que la propia inexistencia constituye, y que, al no existir un esfuerzo gubernamental, no existe un efecto en la prevención o combate de la ciberdelincuencia.

7.2 Fundamentación de lineamientos propositivos .

La investigación realizada por este trabajo fue un esfuerzo en entender las bases doctrinales sobre a la concepción moderna que tenemos sobre el delito informático y su evolución. El marco teórico sirvió para la exploración detallada y el contraste de las posiciones doctrinarias y jurídicas sobre conceptos necesarios para el entendimiento del derecho informático. La aproximación a la doctrina, el análisis de los enunciados bibliográficos expuestos, el análisis jurídico de elementos como la Convención y las campañas de concientización de la INTERPOL, la exploración por contraste del estudio comparativo de legislaciones y la formulación de conclusiones a partir de las mismas, fueron todos aportes que se consolidaron dentro del marco y que sirvieron como base inamovible de la fundamentación de este Trabajo de Integración Curricular, y como fundamentación de los lineamientos propositivos a ofrecer.

Los elementos específicos que fundamentan las proposiciones a plantear más adelante encontraron su virtud de existencia y justificación en los problemas identificados en relación con el estudio previo. De la Jurisdicción, y la exploración del principio de no intervención, se pudo sintetizar como argumento que la acción unilateral de la justicia de un país sobre otro es

inconcebible en estos tiempos, y gracias a cuestiones relacionadas con la eficiencia, se llegó al convencimiento de que acuerdos como el Convenio son grandes herramientas en la cooperación internacional eficiente.

De la exploración de los conceptos informáticos se pudo evidenciar la disparidad temporal entre la norma y la realidad tecnología. Esta no es una noción que se pueda pretender enmendar, ya que mientras las leyes sean un producto del debate democrático, no podrá haber tal cosa como una norma evolutiva. No obstante, eso no salva la obligación de tratar de achicar la brecha. Misma razón por la cual, en los lineamientos propositivos se expondrá respecto de mejoras de necesidad próxima que deben ser incluidas en la legislación con el fin de generar vacíos legales.

Entendiendo que la columna vertebral de la aplicación de la ley se encuentra en el mecanismo coercitivo, representado domésticamente en la Policía Nacional, y la persecución de los actos penalmente punibles, responsabilidad de fiscalía general del Estado. Se contemplo que cualquier tipo de mejora u optimización en los procesos relacionados a los delitos informáticos debería atender la capacitación adecuada estas instituciones con gran preocupación ya que son estas la piedra angular del sistema de justicia penal y del manejo de la cadena de custodia.

En el ejercicio del estudio comparativo, la legislación colombiana resalto por sobre todas las escogidas para estudiar, por encontrarse aún vigente a pesar de haber sido aprobada más de una década atrás. En su uso de los términos generales, el lenguaje técnico adecuado y la incorporación de los datos como sujeto de protección de la ley penal como bien jurídico tutelado, es decir, no se considera la afectación de los datos de una persona por ser de la persona, sino por característica intrínseca de que son datos que han sido vulnerados. Esto sobre la base de que enmarcarlo como un bien jurídico, impregnamos de un valor autónomo a los datos, permitiendo que estos puedan ser sujetos de protección aun cuando estos no perteneciesen a ningún particular o persona jurídica, es decir su protección se garantiza más allá de la afectación que el agravio contra ellos pueda tener sobre un titular.

Evaluando tanto en el marco teórico, como en las opiniones vertidas en las entrevistas realizadas a los profesionales, que la ley es una idea que requiere de la actuación del aparato estatal para materializarse, y que por tanto una buena legislación solo será buena en la medida que los mecanismos de aplicación de esta sean efectivos. Se plantea la necesidad de una posición autocritica de los mencionados mecanismos, sean estos en la Función Judicial o Fiscalía, sobre el valor de sus actuaciones en el campo informático, y la correcta implementación de cambios que

garanticen que el sistema y academia judicial brinden los sistemas y mecanismos para el correcto ejercicio de cualquier tipología que se subscriba en el Código Orgánico Integral Penal, tanto a presente como a futuro.

8. Conclusiones

- Se puede concluir por el estudio jurídico que la legislación penal ecuatoriana ha logrado modernizarse parcialmente a las necesidades tipológicas para la persecución de delitos informáticos en los últimos años. Sin embargo, debido a la falta de caracterización de ciertas modalidades habituales como la estafa informática, la responsabilidad penal culposa en información personal tanto por parte de administradores privados como de públicos, la responsabilidad en la recolección y venta no autorizada de datos recolectados por dispositivos, los usos de criptomonedas para el lavado de activos y la evasión fiscal, y la no contemplación de la Inteligencia Artificial como una modalidad única del delito informático con elementos muy diferentes, se concluye que se requiere aun un esfuerzo legislativo para poder tipificar estos nuevos elementos integrados en las actividades delictivas modernas.
- Se concluye a través del estudio de las estadísticas, que los esfuerzos de modernización de la legislación llevados han tenido un impacto considerable, aunque no suficiente, en la disminución del fenómeno de la ciberdelincuencia
- Se concluye también que existe una carencia completa de Políticas Públicas dirigidas a combatir de la delincuencia informática por parte del Gobierno Central, tanto en prevención como en disuasión o concientización, y una desactualización perjudicial respecto de aspectos informáticos para los miembros operativos de la fuerza pública.
- Se concluye de las entrevistas, encuestas y estudio de casos, que el personal de relacionado con la justicia se encuentra preocupantemente infracapacitado para poder atender adecuadamente las particularidades que el delito informático requiere para su adecuada persecución y las necesidades indispensables en el manejo de los mecanismos probatorios informáticos. Esto incluye a operativos de la policía, peritos y agentes fiscales.
- El estudio de legislación comparada ha concluido que la legislación ecuatoriana ha encontrado en su modernización y nuevas tipologías una mejora sustancial que la expone como un cuerpo jurídico penal que destaca por la implementación de terminología técnica

moderna. Aunque esta puede llegar a ser excesiva en el uso de tecnicismos muy específicos, dificultando así que posibles conductas futuras se acoplen al texto, volviéndolo vulnerable a la obsolescencia. Siendo así una espada de doble filo.

- Se concluye por las opiniones expresada por los especialistas, las encuestas de los profesionales de derecho y el análisis del documento, que la adhesión al Convenio de Budapest es necesaria para concebir no solo un marco jurídico más adecuado, sino también dotar a la justicia de cooperación internacional, ya que la internacionalidad se confirmó como una problemática significativa en la persecución de la cibercriminalidad.

9. Recomendaciones

1. A presidencia de la República y sus ministerios; hacer uso de las facultades constitucionales que le han sido investidas para el ejercicio de la política pública. Servirse de tomar como ejemplo las campañas de concientización e información ya estructuradas e implementadas por la INTERPOL, concientizar a los ciudadanos respecto de los mecanismos que les ofrece la ley y contemplar la seguridad informática dentro del Plan Nacional de Seguridad Integral.
2. Al Ministerio de Educación, se le recomienda incorporar dentro de los planes de estudio una materia orientada a la protección de datos de los propios estudiantes con la que sean capaces de protegerse.
3. Al Consejo de la Judicatura, implementar una pronta reforma a los reglamentos pertinentes y procedimientos respecto del manejo de las pruebas, para que estos contengan provisiones claras y efectivas sobre el manejo de los medios probatorios cuando estos fuesen datos, electrónicos o de carácter informático. A sí mismo, implementar programas de capacitación especializada sobre los elementos de la prueba digital.
4. A las Gobernaciones Provinciales, implementar campañas de concientización y capacitación sobre la importancia de la seguridad y las precauciones en las redes para las poblaciones menos familiarizadas con la informática y grupos vulnerables.
5. A la ARCOTEL, el tomar una posición más proactiva respecto de las restricciones sobre sitios que puedan contener en sus servidores material pornográficos de carácter infantil y simulaciones.
6. A la Asamblea Nacional del Ecuador, redactar y aprobar con celeridad la Ley de creación de la Superintendencia de Protección de Datos Personales.

9.1 Lineamientos propositivos

Este trabajo de investigación propone como lineamientos propositivos lo siguiente:

Se indica a la República del Ecuador, en los poderes públicos de la Asamblea, Corte Constitucional y Presidencia, la urgencia en adherirse al Convenio de Cibercriminalidad de Budapest, con el objetivo de contar con un marco común con el resto de los países participantes y consolidar un protocolo de cooperación internacional eficaz.

Se indica a la Asamblea la necesidad de tipificar ya sea por ley reformatoria, o por proyecto propio, normativas que regulen tecnologías emergentes y de futura adopción como a la inteligencia artificial, las criptomonedas, el Blockchain y demás derivadas de la Web 3.0.

Se propone también que se hagan cambios a los términos de los actos lesivos contra la propiedad intelectual y los derechos de autor para que estos contemplen términos claros sobre la distribución en vivo de contenido sujeto a derechos de autor en redes sociales, y delimitar los límites del uso del contenido tomando como referencia el Fair Use.

Se propone a Policía Nacional la implementación de una capacitación, a nivel de toda la organización, sobre el manejo de pruebas relacionados con datos, electrónica e informática con el fin de evitar la contaminación de las mismas.

Se propone a la Asamblea Nacional, el incorporar al código penal como bien jurídico tutelado a los datos personales y la identidad en las redes;

A Presidencia de la República se le propone la implementación de una campaña nacional de concientización en tres ejes, medios de protección de datos para los ciudadanos, concientización acerca de los tipos vigentes en el Código Orgánico Integral Penal y las formas de acercase a Fiscalía en ayuda, y una campaña de prevención de todas las formas de fishing enfocada a menores de edad, niños, niñas, y de tercera edad. Además, se le propone a Presidencia buscar convenio con empresas desarrolladoras de software técnico en dos puntos, el primero para poder dotar al estado de software de seguridad eficientes que garanticen la protección de los datos de los ciudadanos; el segundo, negociar licencias especiales para los ciudadanos de la república a precios asequibles o becados para el acceso a infraestructura de software necesaria para el mundo laboral digital.

Al Consejo de la Judicatura, se le propone la creación de tribunales especializados para el juzgamiento de estos delitos informáticos, que cuente con jueces que tengan conocimiento especializado respecto de la naturaleza de estos delitos.

A Fiscalía General del Estado se le propone apresurar la consolidación de la Fiscalía

especializada sobre ciberdelincuencia y delitos informáticos, establecida Resolución No. 34 FGE-2022, con los respectivos cambios que se requieran para el efecto en las mallas de capacitación de la Escuela de la Función Judicial por parte del Consejo de la Judicatura.

10. Bibliografía

Aboso, G. E., & Zapata, M. F. (2006). *Cibercriminalidad y derecho penal: la información y los sistemas informáticos como nuevo paradigma del Derecho penal: análisis doctrinario, jurisprudencial y su derecho comparado sobre los denominados delitos informáticos.* B de F.

Aguilar, P. (2015). *¿Derecho informático o informática jurídica?*. Universidad Autónoma de México.

Alban Gómez, E. (2016). *Manual de Derecho Penal Ecuatoriano*. Ediciones Legales. Ecuador.

Altmark, D & Quiroga, E. (2012). *Tratado de Derecho Informático, Tomo I.* Recuperado de https://www.academia.edu/37287922/DANIEL_RICARDO_ALTMARK_EDUARDO_MOLINA_QUIROGA_Colaboradores_acad%C3%A9micos

Anónimo. (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*. ERREIRUS. Recuperado de https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Anónimo. (2022). *Mensaje de datos: ¿Cómo se definen y cuáles son sus tipos?*. DocuSign. Recuperado el 14 de noviembre de 2022 de https://www.docusign.mx/blog/mensaje-de-datos

Arias Ferrer, M. I. (2008). *La Ley sobre Mensajes de Datos y Firma Electrónica: Comentarios a la Sentencia de fecha 12 de febrero de 2008.* Frónesis.

Banco Bilbao Vizcaya Argentaria. (2019). *"Machine Learning" ¿Qué es y cómo funciona?*. Recuperado de https://www.bbva.com/es/innovacion/machine-learning-que-es-y-como-

funciona/

Becares, B. (2023). *Elon Musk lleva años jugando con el precio de Dogecoin. Unos inversores lo demandan por perder grandes cantidades de dinero*. Genbeta portal web. Recuperado de https://www.genbeta.com/actualidad/durante-anos-elon-musk-jugo-precio-dogecoin-unos-inversores-demandan-perder-grandes-cantidades-dinero

Beekman, G. (2005). *Introducción a la Informática*. Pearson Education. Madrid.

Belcic, I. (2016). *¿Qué es un gusano informático?.* Avast. Recuperado 14 de noviembre de 2022 de https://www.avast.com/es-es/c-computer-worm

Belcic, I. (2019). *¿Qué es el Malware?*. Avast. Recuperado el 14 de noviembre de 2022 de https://www.avast.com/es-es/c-malware

Benítez, I. (2015). *El principio de no intervención: consagración, evolución y problemas en el Derecho Internacional actual*. Recuperado de https://www.scielo.cl/scielo.php?pid=S0718-00122015000100013&script=sci_arttext

Berzal, F. (s. f). *Introducción a la Informática*. Recuperado de http://elvex.ugr.es/decsai/JAVA/pdf/1A-intro.pdf

Borja Jiménez, E. (2003). *Sobre el concepto de política criminal. Una aproximación a su significado desde la obra de Claus Roxin*. Anuario de Derecho Penal y Ciencias penales.

Cabanellas, G. (2000). *Diccionario Enciclopédico Jurídico*. Heliasta.

Carnaval Palacios, J. (2008). *Manual de Propiedad Intelectual*. Universidad del Rosario.

Carranza, E. (1994). *Criminalidad ¿Prevención o promoción?*. Universidad Nacional de Educación a Distancia.

Centro de Formación Estudio Criminal. CFEC. (2019). *Definición de la Criminalidad*. Recuperado de https://www.estudiocriminal.eu/blog/definicion-de-criminalidad/

Chichizola, M. (2013). *El Concepto de Jurisdicción*. Universidad del Salvador. Recuperado de https://p3.usal.edu.ar/index.php/aequitas/article/view/1389/1757

Código Orgánico de la Función Judicial. (2009). República del Ecuador.

Código Orgánico Integral Penal. (2014). República del Ecuador.

Código Penal de la Nación. (1921). República Argentina.

Computerworld. (s. f). *Historia de los sistemas operativas*. Recuperado de https://www.computerworld.es/archive/historia-de-los-sistemas-operativos

Comply Advantage. (2023). *Cryptocurrency Regulations Around The World*. Recuperado de https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia.*

DataScientest. (2022). *Inteligencia Artificial: definición, historia, usos, peligros*. Recuperado de https://datascientest.com/es/inteligencia-artificial-definicion

De la Cuadra, E. (1996). *Internet: Conceptos Básicos*. Cuadernos de Documentación Multimedia.

De Pablos, C., et al. (2004). *Informática y comunicaciones en la empresa.* ESIC Editorial. Universidad Rey Juan Carlos

De Pablos, C., et al. (2004). *Organización y transformación de los sistemas de información en la empresa.* ESIC editorial. Universidad Rey Juan Carlos.

Del Pino, A. (s. f). *Delitos Informáticos: Generalidades*. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Ecuavisa. (2021). *Más de 1.200 investigaciones por delitos cibernéticos se registran en Ecuador.* Recuperado de https://www.ecuavisa.com/noticias/mas-de-1200-investigaciones-por-delitos-ciberneticos-se-registran-en-ecuador-MF766709

El Universo. (2020). *Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro.* Recuperado de https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador/

Espinel, C & Bolaños, D. (s. f). *El mensaje de Datos como Evidencia Digital en Colombia*. Universidad Piloto de Colombia.

Estañol, P. (2023). C*hina quiere ajustar la inteligencia artificial a la ideología del Partido Comunista*. Radio Francia Internacional portal web. Recuperado de https://www.rfi.fr/es/ciencia/20230412-china-quiere-ajustar-la-inteligencia-artificial-a-la-ideolog%C3%ADa-del-partido-comunista

Ferrajoli, L. (1997). *Jurisdicción y democracia*. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=174714

Fiscalía General del Estado (2021). *Ciberdelitos. Perfil Criminológico. Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*.

German, J. (2005). *Teorías de Francisco Carrara*. Derecho Ecuador. https://derechoecuador.com/teoriacuteas-de-francisco-carrara/

Gil, J. A. (2017). *El mensaje de datos y su concepción como título ejecutivo en Colombia*. *Revista CES Derecho*.

Harris, J. (2021). *AI advances, but can law keep up?.* Medium. Recuperado

https://towardsdatascience.com/ai-advances-but-cat-the-law-keep-up-7d9669ce9a3d

Hernández Díaz, L. (2009). *El delito informático*. Recuperado de https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

Hernández, L. (2023). *La UE aprueba la regulación sobre las criptomonedas y obliga a las plataformas a identificar a sus clientes*. CincoDías portal web. Recuperado de https://cincodias.elpais.com/companias/2023-04-21/la-ue-aprueba-la-regulacion-sobre-las-criptos-y-obliga-a-las-plataformas-a-identificar-a-sus-clientes.html

Kaspersky. (s. f). *¿Qué es un Keylogger?*. Recuperado de https://latam.kaspersky.com/resource-center/definitions/keylogger

Kaspersky. (s. f). *¿Qué es un troyano y que daño puede causar?.* Recuperado de https://www.kaspersky.es/resource-center/threats/trojans

Kelleher, A. (2022). *Ley de Moore – Ahora y en el Futuro*. Intel portal web. Recuperado de https://www.intel.la/content/www/xl/es/newsroom/opinion/moore-law-now-and-in-the-future.html#gs.1sepnn

Ley Modelo de CNUDMI sobre Comercio Electrónico. Artículo 2. 12 de junio de 1996.

Ley 1273. (2009). República de Colombia.

Ley 21459. (2022). República de Chile.

Malem Seña, J. (s. f). *Acerca De La Pornografía.* https://dialnet.unirioja.es/descarga/articulo/1051086.pdf

Malwarebytes. (s. f). *Todo sobre Adware*. Recuperado de https://es.malwarebytes.com/adware/

Mariaca, M. (2010). *Introducción Al Derecho Penal*. Universidad San Francisco Xavier.

Martínez, N & Matute, H. (2020). *Discriminación racial en la inteligencia artificial*. The conversation portal web. Recuperado de https://theconversation.com/discriminacion-racial-en-la-inteligencia-artificial-142334

Molinario, D. (2021). *¿Qué es un virus de bomba lógica?.* AVG. Recuperado de https://www.avg.com/es/signal/what-is-a-logic-bomb-virus

Morillas Fernández, D. (2005). *Análisis Dogmático y Criminológico de los Delitos de Pornografía Infantil*. Dykinson S.L. Madrid.

Observatorio Anticorrupción. (s. f). *Casos de Corrupción: Ola Bini*. Recuperado de https://www.observatorioanticorrupcion.ec/casos-de-corrupcion/ola-bini

Organización de las Naciones Unidas. (2021). *Recomendaciones generales en la práctica del Comité para la Eliminación de la Discriminación Racial*. Recuperado de https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhssdA56jenkXI9x8o4ndpgXlRhU3HWxR3odQyn1JZxw2YjMzw1QKcxW%2BFtYQCUGObyTbBgOdKvh5%2BL400w%2FjYAVHt3XKaFOdvnodKiFequhQn

Panda. (s. f). *Backdoor o puerta trasera: qué es*. https://www.pandasecurity.com/es/security-info/back-door/

Panda. (s. f). *¿Cómo funciona un Dialer?*. Recuperado de https://es.malwarebytes.com/adware/

Planeta Ius. (s. f) Fallo Sistex, S.A. c. Olivia, S. A. Valerio. Recuperador de http://www.planetaius.com.ar/fallos/jurisprudencia-s/caso-Sistex-SA-c-Oliva-SA-Valerio.htm

Primicias. (2022). *Ciberdelitos suben un 35% entre noviembre y diciembre.* Recuperado de https://www.primicias.ec/noticias/sucesos/ciberdelitos-suben-navidad-ecuador-guia/

Roa Buendía, J. (2013). *Seguridad Informática.* McGraw Hill Education.

Rodríguez, F. (2013). *Derecho Informático: El derecho en la Era Digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela jurídica del sistema informático*. Universidad Nacional de Córdoba.

Romero Castro, M., Figueroa Morán, G., Vera Navarrete, D., Álava Cruzzaty, J., Parrales Anzúles, G., Álava Mero, C., Murillo Quimiz, A., y Castillo Merino, M. (2018). *Introducción a la Seguridad Informática y el Análisis de vulnerabilidades.* Universidad Estatal del Sur de Manabí.

Seguin, P. (2022). *Spyware: detección, prevención y eliminación*. Avast. Recuperado de https://www.avast.com/es-es/c-spyware

Téllez Valdés, J. (2009). *Derecho Informático*. McGraw Hill Education.

Temperini, M. G. I. (2013). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.* Congreso Nacional de Ingeniería Informática/Sistemas de Información.

Temperini, M. G. I. (2013). *Delitos informáticos en Latinoamérica: Un estudio de derecho comparado. 2da. Parte*. Congreso Nacional de Ingeniería Informática/Sistemas de Información.

Torres, A. (2023). Ola Bini o el juego de los enemigos. Primicias. Recupera de https://www.primicias.ec/noticias/firmas/olabini-juicio-hacker-ecuador-analisis/

Universidad a Distancia de Madrid. (s. f). Cibercriminología. Recuperado de https://www.udima.es/es/cibercriminologia.html

Velasco, J. (2014). *Breve Historia de la Criptografía*. ElDiario portal web. Recuperado de https://www.eldiario.es/turing/criptografia/breve-historia-criptografia_1_4878763.html

Velloso, A. (2015). Jurisdicción y competencia. Recuperado de https://campus.academiadederecho.org/upload/Cvaav/Pdf/NF%20-%20AD/Ad/Jurisdiccion_y_Competencia__AAV.pdf

11. Anexos

11.1 Encuestas dirigidas a profesionales del Derecho

UNIVERSIDAD NACIONAL DE LOJA FACULTAD JURIDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

Preguntas

1. ¿Estima usted que la legislación penal vigente en términos informáticos es suficiente y ofrece los mecanismos procesales y tipos adecuados para la persecución del fenómeno de la ciberdelincuencia?

SI ( ) NO ( )

¿Por qué?

……

……

……

2. En base sobre su experiencia en el campo ¿estima que en ordenamiento jurídico actual es practico y procesalmente viable perseguir acciones informáticas que se desarrollaron en las redes?

SI ( ) NO ( )

¿Por qué?

……

……

……

……

3. ¿Aprecia conveniente a los intereses del Ecuador el adoptar marcos internacionales como mecanismo para modernizar su legislación en cibercriminalidad y delitos informáticos?

SI ( ) NO ( )

¿Por qué?

……

……

……

……

4. ¿Estima usted que el marco jurídico informático actual protege adecuadamente los bienes jurídicos de la privacidad, seguridad y justicia que garantiza la CRE?

SI ( ) NO ( )

¿Por qué?

……

……

……

……

5. ¿Considera que el Gobierno central ha aplicado una política pública criminal que haya aplacado o disminuido los delitos informáticos y la cibercriminalidad?

SI ( ) NO ( )

¿Por qué?

……

……

Anexos 1. Encuestas dirigidas a profesionales del Derecho

11.2 Entrevistas Dirigidas a Profesionales de Derecho

UNIVERSIDAD NACIONAL DE LOJA FACULTAD JURIDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

Preguntas

1. **¿Qué opinión le merece usted el estado actual de la legislación penal informática tipifica dentro del Código Orgánico Integral Penal?**
2. **¿Encuentra que los mecanismos de persecución formalmente configurados en elordenamiento actual son procesalmente eficientes y eficaces?**
3. **¿Ha encontrado usted dificultades procesales al momento de encausar un delito concarácter informático? ¿Cuáles fueron estas dificultades?**
4. **A su criterio personal ¿Que le faltaría implementar o modificar a la política criminaldel Gobierno central para combatir y prevenir los delitos informáticos?**
5. **El Estado ecuatoriano no se encuentra subscrito al Convenio de Ciberdelincuencia de Budapest ¿Estima usted que la no adhesión al convenio ha perjudicado el esfuerzo enla percusión de la justicia en el ámbito informático?**
6. **A su experiencia en el campo sobre los delitos informáticos ¿Qué lineamientos estima necesarios en implementar dentro del ámbito jurídico ecuatoriano para poder solventarlos mencionados problemas?**

Anexos 2. Entrevistas dirigidas a Profesionales

11.3 Certificado de Traducción de Idioma Ingles

Loja, 28 de Junio de 2023

Jennifer Karla Ortega Vegas

Licenciada en Pedagogía del Idioma Ingles

CERTIFICO

Que he realizado la traducción del resumen de la tesis titulada "**LA PROBLEMÁTICA DE LOS DELITOS IFORMATICOS EN EL ECUADOR, SU PERSECUCION Y CAPACIDAD PREVENTIVA DE LA LEGISLACION ECUATORIANA EN CONSTRASTE CON EL DERECHO COMPARADO**" del idioma español al idioma inglés, presentado por **JOE SEBASTIAN CONTENTO MARTINEZ**, portador de la cedula de identidad: **1950032969**, como requisito para obtener el título de Abogado de la Universidad Nacional de Loja.

Por medio del este certificado, aseguro que la traducción del resumen de la tesis ha sido realizada de acuerdo con los estándares y prácticas de traducción vigentes, y que el resultado final es una versión precisa y comprensible del documento original.

Lic. Jennifer Karla Ortega Vega

Registro de Senecyt No: 1800-2023-2679944

Correo: jk.ortega@gmail.com

Anexos 3. Certificado de Traducción de Idioma Ingles