UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIVERSIDAD CATÓLICA DE CUENCA

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA: ANÁLISIS DE LA FALTA DE TIPIFICACIÓN DE LA CONDUCTA: *RANSOMWARE* (SECUESTRO DE DATOS) EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPUBLICA

AUTOR: FREDI GUSTAVO JARA CABRERA

DIRECTOR: AB. BERNARDO XAVIER MONSALVE ROBALINO MGS.

CUENCA - ECUADOR

2022

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES

CARRERA DE DERECHO

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA

Análisis de la falta de tipificación de la conducta: Ransomware (Secuestro de Datos) en el Código Orgánico Integral Penal.

AUTOR: Fredi Gustavo Jara Cabrera

DIRECTOR: Ab. Bernardo Xavier Monsalve Robalino Mgs.

CUENCA - ECUADOR

2022

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Universidad Católica de Cuenca	DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

Fredi Gustavo Jara Cabrera, portador de la cédula de ciudadanía N.º **0105120265**. Declaro ser el autor de la obra: **"Análisis de la falta de tipificación de la conducta: Ransomware (Secuestro de Datos) en el Código Orgánico Integral Penal"**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, 06 de septiembre de 2022.

F: .....

Fredi Gustavo Jara Cabrera

C.I. **0105120265**

CERTIFICADO DE TUTOR

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por Fredi Gustavo Jara Cabrera, con el tema **Análisis de la Falta de Tipificación de la Conducta: *Ransomware* (Secuestro de Datos) en el Código Orgánico Integral Penal** bajo mi supervisión.

Ab. Bernardo Xavier Monsalve Robalino
Tutor

DEDICATORIA

El presente proyecto de investigación está dedicado a mi padres, Diana y Fredi, ya que gracias a su apoyo y motivación pude sobrellevar los obstáculos que se presentaron en el proceso para alcanzar esta meta, y hasta este punto de mi vida en general. Este trabajo de investigación lo realizo en nombre de todo el esfuerzo y sacrificio entregado a lo largo de estos años por su parte para hacer posible esta realidad, los cuales me han hecho valorar en gran medida el tener un apoyo incondicional con el cual contar a pesar del paso de los años y de las situaciones.

AGRADECIMIENTO

A través de este trabajo de investigación quiero hacer un agradecimiento a los catedráticos que fueron parte del proceso de formación académica que recibí dentro de esta prestigiosa universidad, quienes a lo largo de las clases impartidas supieran sembrar en nuestras personas conocimientos de calidad, valores y las ganas de servir a la sociedad, lo cual ha motivado a mi persona a ser un sujeto de bien en la práctica profesional y en la vida en general.

De igual manera, quisiera extender un agradecimiento a mi tutor, el Ab. Bernardo Xavier Monsalve Robalino, catedrático de la Universidad Católica de Cuenca, ya que gracias a su seguimiento y tutela a lo largo del proceso de elaboración de este proyecto fue posible el realizar una investigación de calidad y obtener resultados de la misma que aporten a la sociedad con una iniciativa de cambio, con propuestas creadas con bases científicas sólidas que aborden la problemática desarrollada y ofrezcan una solución hacia la misma.

Además, hago un agradecimiento a mi familia: mis padres, Diana y Fredi, mis hermanos, Karen y Rafael, y a todas las personas que me brindaron su compañía y apoyo de manera incondicional a lo largo de este proceso de crecimiento tanto personal como profesional.

INDICE

RESUMEN

El presente Trabajo de Investigación abarca la problemática de la regulación de los delitos informáticos en nuestro ordenamiento jurídico, con énfasis en el estudio de la tipificación de la conducta de *Ransomware* (Secuestro de Datos) a partir de una investigación de enfoque cualitativo de doctrina, legislación nacional, legislación comparada, y de Tratados y Convenios Internacionales ratificados por el Estado ecuatoriano referentes a Delincuencia Informática. Se determinan los conceptos y definiciones de Derecho Informático, Derecho Penal Informático, la modalidad de ejecución de los Delitos Informáticos propiamente, de la conducta *Ransomware*, sus elementos, características, y una clasificación de aquellos que son los más suscitados según análisis de juristas especializados en la materia, además del análisis de la "Funcionalidad Informática" como nuevo bien jurídico protegido, según la doctrina, estableciendo un mejor contexto del fenómeno a estudiarse; seguido de la elaboración de un análisis del Tipo Penal de los artículos del Código Orgánico Integral Penal que tienden a regular las conductas que llegan a definirse como "Delito Informático" con el fin de identificar los aspectos que regula el Código, y los que no, ante estas conductas; para finalmente determinar si se regula o no esta conducta por medio de una contrastación de los resultados obtenidos en los capítulos desarrollados y de la información investigada.

PALABRAS CLAVES: Cibercrimen, Protección de Datos, Informática, Secuestro de Datos.

ABSTRACT:

This research work covers the problem of the regulation of computer crimes in our legal system, with emphasis on the study of the criminalization of the behavior of *Ransomware* (Data Hijacking) from a qualitative research approach of doctrine, national legislation, comparative legislation, and International Treaties and Conventions ratified by the Ecuadorian State concerning computer crime. The concepts and definitions of Computer Law, Computer Criminal Law, the modality of execution of Computer Crimes itself, *Ransomware* behavior, its elements, characteristics, and a classification of those that are the most frequent according to the analysis of jurists specialized in the matter, and the scrutiny of the "Computer Functionality" as a new protected legal good —according to the doctrine— are determined to establish a better context of the phenomenon to be studied. An analysis of the Penal Type of the articles of the Organic Integral Penal Code that tend to regulate the conduct defined as "Computer Crime" is elaborated to identify the aspects that the Code does and does not regulate. Finally, it is determined whether this behavior is regulated or not by contrasting the results obtained in the developed chapters and the investigated information.

KEYWORDS:

Cybercrime, Data Protection, Informatics, Data Hijacking.

INTRODUCCIÓN

La sociedad y el ser humano a lo largo de las últimas décadas han sufrido una serie de cambios que han desencadenado que eventos como la automatización y la inclusión de la tecnología en actividades cotidianas de las personas en procesos de educación, socialización, educación, entre otros, provoquen una preocupación para el Derecho que crece a medida que la ciencia y la creación e innovación de la tecnología se desarrollan cada vez más, dando lugar a una serie de conductas que pueden desembocar en detrimentos hacia los derechos de otras personas, y que a costa de este daño se pueda obtener cierto beneficio para el autor o autores.

Con el tiempo se han llegado a identificar ciertos patrones en este tipo de hechos que permiten a los expertos informáticos encuadrarlas a diversas clases de ilícitos con nombres propios de acorde a su función o modo de realización, como el *phishing*, *pharming*, y el *ransomware*, los cuales serán estudiados a su debido momento, que son conductas cuyos términos fueron acuñados de acorde a la forma en la que se cometen, y con la ayuda de compañías desarrolladoras de *software* antivirus se han podido tomar ciertas medidas que ayudan para reducir en cierto grado estos ataques informáticos, que puede resultar en un problema molesto para una persona en particular, para compañías o entidades víctimas de ataques, o para el mismo Estado al momento en el que instituciones y dependencias públicas se vean afectada de cualquier forma por la presencia de Delitos Informáticos.

El Secuestro de Datos o Ransomware pertenece a esta categoría de Delitos Informáticos que contempla la doctrina, basados en la comisión de los mismos por medio de sistemas informáticos en contra de otros del mismo tipo y que afectan a las

funciones lógicas del sistema operativo, los cuales habían sido ajenos al análisis del Derecho al tomarse en cuenta únicamente aspectos materiales y en la información de los sistemas u ordenadores afectados para la creación de normativa, y que hoy en día han llegado a tener la misma importancia entre sí para la creación de bases doctrinarias y para el desarrollo de los ordenamientos jurídicos que regulan esta problemática.

A lo largo de este trabajo de investigación se desarrollarán tres capítulos: el primer capítulo basado en el método de revisión documental, en el que se abarcarán todos los aspectos doctrinarios de los Delitos Informáticos, Derecho Penal Informático, y de la conducta de *Ransomware* (Secuestro de Datos) conjuntamente con sus elementos, características principales y su clasificación; el segundo capítulo, el mismo que es realizado con el método Análitico-Sintético contendrá un análisis del Tipo Penal de los Delitos Informáticos contenidos en la regulación del Código Orgánico Integral Penal con el fin de determinar la situación del ordenamiento frente a nuevos delitos relacionados con el uso de nuevas tecnologías y sistemas informáticos; y el tercer capítulo, desarrollado a partir del método Inductivo-Deductivo estará basado en la contrastación de la información obtenida en los capítulos previos, con el fin de determinar si nuestra legislación regula o no la conducta de Secuestro de Datos.

Al final se realizarán una serie de recomendaciones basadas en la información obtenida del presente proyecto, las cuales estarán encaminadas a dotar al Estado de una solución debidamente fundamentada hacia la problemática que rige sobre el Secuestro de Datos como Delito Informático.

1. Capítulo I: Delitos Informáticos y *Ransomware*

1.1. Conceptos y Definiciones

Primeramente, hay que establecer los conceptos básicos y definiciones de los temas a abordarse, tal como lo es el Derecho Penal, el Derecho Informático, el Delito Informático y los delitos informáticos más suscitados. Hay que hacer referencia de cuáles de ellos son los que afectan más a la población, con hincapié en el *Ransomware* o Secuestro de Datos con sus elementos y modalidad de funcionamiento con el objetivo de obtener datos sobre el campo de estudio al cual nos adentramos y poseer una visión completa de la problemática a enfrentarse, teniendo claras todas las nociones básicas que involucran al *ransomware* para un tratamiento jurídico correcto.

1.1.1. Derecho Penal

El Derecho es aquel grupo de reglas coordinadas que regulan la conducta de la sociedad humana, y lo Penal hace referencia a cualquier situación en la que una acción cometida maliciosamente desemboca en un castigo o Pena; por lo tanto, el Derecho Penal es aquel conjunto ordenado de reglas, normas y principios que tienden a regular las conductas catalogadas como infracciones y que imponen una sanción en el caso de ser cometidas. (Bacigalupo Saggese et al., 2019, p.28)

Según Solano Vélez et al. (2019) el Derecho Penal es aquel conjunto de leyes y normas que otorgan una pena, castigo o medida a una conducta categorizada como punible. Esta acción que busca ser castigada con el uso del poder punitivo debe encontrarse tipificada en la normativa para que surta efecto en su totalidad, de lo contrario, si algún acto no está clasificado como una infracción no podrá ser castigado

ni se podrá emplear una medida para cesar o prevenir dicha situación cuando se presente. (p. 118)

Con las definiciones esgrimidas de estos autores podemos entender que el Derecho Penal es el conjunto de normas, reglas y principios jurídicos que tienen por objeto regular, prevenir y sancionar aquellas conductas realizadas en contra de otra persona o grupo de personas y que se encuentren reguladas dentro del catálogo de delitos del ordenamiento jurídico, haciendo un claro énfasis en el principio de Legalidad, en que si una acción no está tipificada no se podrá emprender ninguna acción penal para su cese o mitigación.

1.1.2. Derecho Informático

La ciencia de la Informática puede ser definida como aquella que, mediante el uso de ordenadores y sistemas de procesamiento de información, estudia los procedimientos de tratamiento de información, desde su creación, almacenamiento y transmisión entre servidores u otros usuarios, con sustento tanto teórico como práctico para determinar la eficacia de dichas técnicas de tratamiento de datos.

El Derecho Informático se presenta como una rama innovadora del Derecho que tiende a regular el fenómeno social que se ha producido debido al avance de la tecnología y su implementación en el vivir cotidiano del ser humano; el Derecho Informático y su incorporación en la sociedad desencadenan una serie de consecuencias a nivel social, político, económico y jurídico, ya que al estar presentes los sistemas informáticos y computadoras en estos ámbitos de la sociedad por ende se emplearán regulaciones para controlar su uso. (Téllez Valdés, 2009)

Esta rama del Derecho tiende a ser un mecanismo dinámico que tiene por objeto el normar el uso de la tecnología y los aparatos electrónicos dentro de la sociedad, puesto que forman parte de ciertos servicios que se usan de manera cotidiana como los servicios bancarios y de pagos, de comida, empresariales, judiciales, entre otros. Sin embargo, de entre el Derecho Penal y el Derecho Informático surge una rama de estudio centrada en el estudio de las infracciones penales cometidas a través de medios tecnológicos y de sistemas informáticos, siendo esta rama concebida como Derecho Penal Informático. A través de este Derecho Penal Informático el Estado debe optar por medio de sus legisladores por ofrecer una regulación de delitos informáticos tipificados en base a estudios con expertos informáticos que puedan aportar con pautas para la creación de las diversas regulaciones encargadas de enfrentar dicho fenómeno, teniendo así la aplicación de varios campos de estudio que complementan al jurídico y al desarrollo de doctrina, leyes y jurisprudencia.

1.1.3. El Derecho Penal Informático

Al pretender ser un campo nuevo de acción dentro del Derecho Penal tradicional, el Derecho Penal Informático surge como una rama del Derecho Público dedicada al desarrollo de doctrina, medidas y directrices para lidiar con la aparición de los delitos informáticos, fenómeno que se ha dado lugar conjuntamente con el *boom* de la internet, la globalización y la adopción de la sociedad un estilo de vida notablemente automatizado. El objeto de su creación es el de determinar los nuevos bienes jurídicos protegidos que se ven menoscabados en esta clase de delitos, diferenciando así los delitos clásicos que afectan a la integridad física, psicológica o sexual del ser humano o

su patrimonio, entre otros, de esta clase de delitos relativamente nueva. (Espinoza Coila, 2018)

Dicho de otra manera, el Derecho Penal Informático es una rama del Derecho Penal que tiene la finalidad de regular y de sancionar aquellas conductas que desemboquen en el daño de los sistemas operativos (*software*) de las víctimas o de la información contenida en sus bases de datos y que pueda afectar la disponibilidad que el usuario posee sobre ella, dando como resultado la afectación de nuevos bienes jurídicos, como la funcionalidad de dichos sistemas, las bases de datos, y entre otros elementos que el Derecho Penal tradicional no podría regular a cabalidad debido a su naturaleza doctrinaria.

1.1.4. Concepto y Definiciones de los Delitos Informáticos

Zambrano Pasquel (2021) nos explica que un delito es aquel acto de interés para el Derecho Penal, que es antijurídico, culpable y que puede contener dolo o culpa, elementos indispensables para el poder punitivo al momento de establecer si la acción u omisión realizada es voluntaria o proviene de la involuntariedad, ya que de no ser el caso de cumplir con estos requisitos dicha conducta no puede ser tratada con medidas del Derecho Penal. (p. 203)

Fuentes Marrufo et al. (2017) establecen que por delito informático “suele entenderse toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.” (p. 2); y en cuanto a otro concepto se dice que “el delito informático puede ser conocido como delitos telemáticos, crímenes virtuales, cibercrímenes, ciberterrorismo, entre otros.”. (Acosta et al., 2020, p. 5)

Podemos destacar que estos delitos se caracterizan principalmente por valerse del uso de medios informáticos y ordenadores como herramienta para el cometimiento de la conducta, por afectar a bienes jurídicos relacionados con la tecnología y el derecho de las personas a su acceso y uso, por lo que someramente se podría definir a un delito informático como una conducta punible, antijurídica y culpable que es cometida por medio de sistemas informáticos.

La ciberdelincuencia y los delitos informáticos son un problema que tiene su auge en las últimas décadas, principalmente tras la culminación de la guerra fría y la aparición de la internet como una herramienta novedosa y accesible en cualquier actividad del ser humano moderno. Diversos Estados tomaron este escenario como un riesgo para sus ordenamientos, por lo que optaron por la elaboración de Convenios y Pactos para poder crear una doctrina y regulaciones uniformes sobre lo que se trataría como “delito informático”; en estos acuerdos se lo define como cualquier acto ilícito en el cual el empleo de un sistema informático, ordenadores o tecnologías aplicadas a la comunicación e información es vital para su realización y su finalización. (Gonzales et al., 2018)

Según Mayer Lux (2018) los delitos informáticos deben ser estudiados y analizados conjuntamente con otras áreas de conocimiento ajenas al Derecho y no únicamente depender de criterios estrictamente jurídicos para crear una regulación eficaz en el tema, puesto que en el presente caso notamos que es menester la intervención de la Informática como complemento doctrinario y científico para un debido tratamiento de esta problemática dentro de la legislación y en la sociedad. Esto es indispensable para obtener una mayor comprensión sobre el acelerado paso al que va

la evolución de Informática y la creación de nuevos sistemas, del idioma o codificación utilizada para su programación, llegando a ser necesario el poseer cierto nivel de conocimiento en dicha área para comprender en su totalidad las operaciones que se realizan y para precisar de una forma más efectiva las conductas que se pretenden introducir en la normativa penal (p. 160)

Por otra parte, si analizamos el contexto de la emergencia sanitaria producida por la pandemia del virus COVID-19 en cuanto al desarrollo de la Informática, los ordenadores, redes sociales y servicios en línea contratados bajo suscripción durante este periodo podremos notar que se ha obtenido un crecimiento en la creación de aplicaciones, plataformas en línea y un aumento en los usuarios de las mismas tras el aislamiento adoptado por la Organización Mundial de la Salud como medida para la erradicación de la infección, dando como resultado una serie de consecuencias a nivel psicológico y social en las personas, generando dependencia al uso de la tecnología, nuevas conductas delictivas además de incrementar las ya existentes de las cuales podemos resaltar a las estafas electrónicas que han venido produciéndose desde hace algunos años, y el *phishing*, *pharming*, *ransomware,* entre otras conductas cometidas mediante *malware* y con el uso de ordenadores, como actos relativamente novedosos en su modalidad de operación y en los medios a través de los cuales son ejecutados. (Macías-Lara et al., 2022)

1.2. Modalidad y Características de los Delitos Informáticos

En este tipo de delitos se utilizan como herramienta principal los sistemas informáticos y son ejecutados por personas expertas en informática. Estos expertos se dan a conocer por nombres como *hackers* y *crackers*; los *hackers* son sujetos expertos

en informática que realizar ciberataques e invasiones a otros ordenadores por simple afición, o sin un fin de beneficio específico; a diferencia de los *crackers*, expertos que pertenecen a bandas delictivas y siempre operan bajo el nombre de estas organizaciones o a manera personal con un ánimo de lucro o de obtener un beneficio en base al daño a terceros. Entre otras características podemos destacar que estos actos son cometidos bajo situaciones previamente planeadas o elaboradas por el sujeto activo en las cuales, en base al engaño, la víctima se predispone a colaborar dejando una brecha en la seguridad de su sistema de manera inducida; pueden ser usados como estrategias de sabotaje a los gobiernos y a sus bases de datos; son conductas que se encuentran latentes en nuestra sociedad y que no se han tipificado en la actualidad. (Saltos Salgado et al., 2021, p. 346)

Una particularidad de estos delitos que cabe analizar es la facilidad que tienen los autores para llevarlos a cabo, dependiendo únicamente del acceso a un ordenador y conexión a una red de internet sin importar el lugar y el momento del día en el que se producen y pudiendo ejecutarse desde una oficina, parques, computadoras de acceso público (ciber cafés, bibliotecas, etc.). Como otro desencadenante de este fenómeno podemos señalar el hecho de que en la actualidad existe una cantidad considerable de aparatos electrónicos en los hogares y que los miembros de éstos se encuentran activamente en consumo de plataformas o cualquier aplicación que involucre tecnologías de la información con conexión a internet, situación que los hace vulnerables a los métodos de engaño de *hackers* para crear una brecha en la seguridad de sus ordenadores y dar paso a estos actos delictivos. (Mayer Lux, 2018)

En definitiva, la modalidad empleada por los autores de estos ilícitos facilita a que se den lugar desde cualquier parte del mundo en cualquier momento, bastando únicamente con tener acceso a la red y los conocimientos necesarios para poder implantar *malwares*, virus o cualquier herramienta informática que desate un sabotaje en el funcionamiento del soporte lógico del ordenador, dando así una serie de problemas para el Derecho y los ordenamientos jurídicos de los Estados que sufren esta clase de delitos por el considerable grado de dificultad que se desprende al determinar los autores, el lugar, la modalidad, herramientas y demás elementos fundamentales para determinar cuestiones como la jurisdicción bajo la cual se juzgarán, las leyes, tratados o convenios aplicables para la resolución del caso, y demás requisitos sustanciales de ley para una correcta resolución de casos.

Como última característica podemos señalar la singularidad de que los usuarios suscritos a plataformas o sitios web que requieren introducir cualquier clase de información, sea personal, académica, financiera, entre otras, son personas que se encuentran en un mayor grado de vulnerabilidad de sufrir secuestros, falsificaciones, cifrados o restricciones a la disponibilidad de dicha información, causado por obra de *hackers* o expertos informáticos anti-éticos; esto se debe a la exposición que tienen dichos sujetos ante los métodos que emplean los piratas informáticos para generar una grieta en la seguridad de sus ordenadores y que se de paso así a un fraude o delito informático. (Villón et al., 2019, p. 235)

1.3. El Bien Jurídico Protegido en los Delitos Informáticos

La jurista Mayer Lux (2017) analiza doctrinariamente a los bienes jurídicos, partiendo por la definición de que son bienes o condiciones de carácter corporal o incorporal que pertenecen a una persona, grupo de personas o entidades y que poseen relevancia para su libre desarrollo dentro del Estado. Estos bienes pueden ser individuales o colectivos. No obstante, el Estado busca la protección tanto de las necesidades colectivas como de las individuales, sin colocar en una posición privilegiada a determinados grupos de personas en cuanto a la tutela y la aplicación de las medidas para dicho efecto, logrando así que todas las personas del territorio puedan tener la misma libertad y oportunidades para su desarrollo personal e individual. Por otra parte, si bien la tutela que se otorga a todos los bienes jurídicos es la misma por parte del Estado, al pertenecer los bienes jurídicos colectivos a toda la población puede generarse una especie de protección y resarcimiento inmediato de cualquier situación que dé como consecuencia la afectación de estos bienes, dado que al ser de propiedad de todos los ciudadanos cualquier menoscabo desembocaría en una privación al libre desarrollo de cada persona y grupos de personas, a diferencia de los bienes jurídicos individuales, que cuando sufren detrimentos provocan consecuencias a nivel del individuo o de un grupo solamente, mas no a la sociedad en general. (p. 236-239)

Al mismo tiempo el profesor Cornejo Arismendi (2021) utiliza como referencia el criterio del profesor Norberto De La Mata para exponer el papel que tiene el Derecho Penal Informático la regulación de infracciones de carácter informático en la doctrina para determinar los nuevos bienes jurídicos a estudiarse, sin desmerecer al Derecho

Penal tradicional y a los que éste tutela, tales como la integridad física, la libertad de la persona, o la vida, considerándose más bien como un complemento del Derecho Penal para abarcar el fenómeno de la tecnología junto con las consecuencias que acarrea su uso. Por consiguiente, al fijar la premisa de que en estos delitos se relaciona directamente a la informática y a los sistemas, estos autores coinciden en que el nuevo bien jurídico protegido es la funcionalidad de los sistemas informáticos. (p. 98)

En síntesis, un bien jurídico es aquel bien material o inmaterial, sea individual o colectivo, que es vital para el libre desarrollo de las personas y que en caso de sufrir detrimentos el Estado está en la obligación de adoptar medidas para su reparación acompañada del resarcimiento del daño causado a la víctima. Ya trazada esta línea, es pertinente mencionar que los delitos informáticos llegan a afectar a un bien jurídico en específico que está relacionado directamente con el funcionamiento de los ordenadores y sus sistemas de soporte lógico, o *softwares*, excluyendo deterioros físicos o del *hardware* de dichos equipos de entre otras conductas que tengan como consecuencia un daño material en los equipos donde los sistemas informáticos operan.

El bien jurídico protegido que se violenta en esta conducta llegaría a ser la *funcionalidad informática*, determinada como el correcto funcionamiento y uso de las tecnologías aplicadas a la comunicación y de tratamiento de información por medio de sistemas informáticos u ordenadores en pro de las personas que emplean estas tecnologías para desenvolverse en su vida en todos los ámbitos que sea posible, siendo un bien jurídico inmaterial de carácter colectivo por el derecho de las personas de acceder a ellas sin restricciones de ninguna clase, asimismo de poder utilizarlas sin

que su integridad, sus derechos o su patrimonio se vea en riesgo alguno. (Mayer Lux, 2017, p. 250-252)

La Funcionalidad Informática es un bien jurídico que puede ser enmarcado como nuevo frente a otros bienes jurídicos como el patrimonio, la integridad física de las personas, entre otros que se afectan en los delitos clásicos, dado que al hacer mención al correcto funcionamiento de los sistemas informáticos, de los procesos que se usan para el tratamiento de la información dentro los mismos, y del derecho de la colectividad de emplearlos a su parecer dentro del marco de la ley, se da a entender que es de mayor importancia la funcionalidad de estos sistemas y los datos que almacenan para las personas que la información así como tal, pues estos datos a simples rasgos no significan nada sin el uso que los individuos les otorguen en la vida.

En este contexto se debe tener en cuenta los derechos humanos que han sido reconocidos en tratados y convenios internacionales, entre los cuales se sitúa el derecho de todas las personas de acceder a medios tecnológicos y de acceder a internet, debidamente reconocidos por la Asamblea General de las Naciones Unidas como efecto del fenómeno social de la incorporación de la tecnología en la cotidianidad de las personas en sus procesos académicos, sociales, laborales, financieros, entre otros, tanto de las personas de escasos recursos como de aquellas que poseen una capacidad económica más estable. Al privar a las personas del goce de estos derechos se está atentando en contra de disposiciones de Organismos y Convenios internacionales, lo cual apoya la posición de que la funcionalidad informática es un bien jurídico colectivo y que se ve directamente violentado por estos actos de ciberdelincuencia. (Villón et al., 2019)

1.4. Delitos Informáticos dentro del Ecuador

Al hablar de delitos informáticos en sentido estricto se debe verificar que se traten de conductas ilícitas cometidas por medio de tecnologías aplicadas a la comunicación e información, soportadas por un sistema operativo, que hacen uso de una conexión a la red, y que se centran netamente en afectaciones a otro sistema lógico o sistema informático, de lo contrario se estaría hablando de delitos en contra de la propiedad, refiriéndonos a cualquier averío inducido en el *hardware*.

Entre los “delitos informáticos” regulados dentro del ordenamiento jurídico se encuentran los sabotajes informáticos, fraudes, el espionaje, actos contra la propiedad intelectual, además de la difusión de material pornográfico de menores de edad, o reproducción de contenido sin consentimiento de la persona a la que pertenece, mostrando así el ordenamiento jurídico un tratamiento sobre esta problemática. (Villón et al., 2019)

Empero, si bien la normativa penal ofrece un catálogo de delitos informáticos, estos no atienden al presupuesto deducido en la presente investigación en tanto a la modalidad de ejecución de los delitos cometidos mediante el uso de sistemas informáticos en contra de la funcionalidad de otro u otros sistemas informáticos. A continuación, se analizarán algunas conductas ilícitas que han sido detectadas dentro del territorio nacional y que cumplen con los presupuestos ya manifestados:

a) Bot Malicioso: es conocido por este término el malware o software malicioso creado e instalado dentro de un sistema operativo por medio de publicidad engañosa de sitios web o correos electrónicos *spam*, que desemboca en un averío en el funcionamiento del sistema al completarse su instalación,

causando pérdida de información parcial o total, además de dejar obsoleto por completo al sistema en el caso en el que el ataque haya escalado a dicho nivel. La descarga que se produce no es voluntaria y el malware se inmiscuye dentro del ordenador de forma inadvertida hasta el momento en el que la víctima del ataque realice dicha situación. (Macías-lara et al., 2022, p. 238)

b) *Phishing:* es una conducta que funciona por medio de correspondencia electrónica y demás correspondencia que involucre el tránsito digital de mensajes de datos. Los delincuentes informáticos se hacen pasar por entidades bancarias, gubernamentales, o por cualquier entidad privada o del sector público, y por medio de estos mensajes envían *links* o instrucciones para que sus víctimas ingresen voluntariamente a estos enlaces, solicitándoles su información tanto de carácter personal, bancario, o cualquier tipo de datos de los que los delincuentes informáticos puedan beneficiarse. Esto resulta perjudicial para la estabilidad de estas entidades, ya que muchos de los afectados por esta conducta descargan sus descontentos con el personal encargado de las mismas, llegando incluso hasta al abandono por parte de sus usuarios a las entidades suplantadas, representando así no únicamente un problema de seguridad o informático netamente, puesto que involucra también a la imagen y prestigio del trabajo de las organizaciones. (Villón et al., 2019, p. 673)

c) *Pharming:* se acuña por medio de este término a la actividad de recolección masiva de información que realizan los delincuentes informáticos por medio

de la suplantación de páginas electrónicas verificadas de empresas, entidades u organizaciones legalmente constituidas. La modalidad de este delito es que, los delincuentes replican páginas web que aparentan ser verificadas (por medio del *Hyper Text Transfer Protocol Secure* o *HTTPS* no confiable de dichas páginas) en las cuales se colocan campos en los que se solicita información determinada que puede ser utilizada para causar perjuicio a su titular y obtener una retribución o beneficio económico con su uso no autorizado. Esta conducta se caracteriza por ser una modalidad con un mayor alcance que el *phishing*, ya que al estar replicadas estas páginas cualquier usuario puede verse en el riesgo de ingresar a ellas desde un buscador, sin la necesidad de ingresar a correos o mensajes de datos para ingresar a las páginas. En pocas palabras el *pharming* es un *phishing* producido de forma masiva. (Villón et al., 2019, p. 673-674)

d) *Ataques DDoS*: este básicamente es un ataque masivo a los servidores que soportan las páginas o portales web, de manera que es una conducta que debe ser cometida por un número considerable de personas, los cuales poseen un orquestador y sujeto que organiza estos ataques. Esta conducta es conocida por ser cometida únicamente en base a la sobrecarga de las páginas, sin que todos los participantes deban ser expertos informáticos, siendo muy fácil de organizar y llevarla a cabo. Esto también provoca que los propietarios de las páginas pierdan acceso a ellas o que los dominios web bajo los cuales está creada la página sean inservibles, debiendo crear nuevos sitios que pueden ser objeto de un futuro atentado. Por otra parte,

esta técnica no es utilizada solo por delincuentes informáticos para causar sabotajes, ya que también es un método efectivo para poner a prueba los servidores y lograr establecer rangos de capacidad y de alojamiento de usuarios. (Romano Ozcáriz, 2019, p. 126-127)

e) *Ransomware:* es el *software* malicioso que es creado a partir de un código malicioso que al ingresar en los ordenadores afectados inmediatamente bloquea la totalidad de de la información contenida en sus bases de datos o únicamente una parte, y solicitando por la liberación o desencriptado de la información una retribución o pago, como en una especie de secuestro informático de datos. Este *malware* es implantado en los ordenadores por medio de ingeniería social, es decir métodos de engaño de los ciberdelincuentes por medio de mensajes electrónicos o de datos, mediante los cuales las víctimas al ingresar en ellos los descargan en sus sistemas involuntariamente, o, dependiendo del tipo de *ransomware,* también puede ser instalado sin el conocimeitno de la víctima sino hasta el momento en el que se produce el encriptado de su ordenador. Existen varios tipos de *ransomware*, clasificándose algunos por su función o por el margen de bloqueo o encriptado que abarquen, dependiendo esto de la creatividad de los expertos informáticos al crear y programar estos virus. (Estrada Cola, 2018)

Como una característica en particular que poseen los delitos enumerados podemos señalar a la llamada “Ingeniería Social”, o el conjunto de técnicas que utilizan los expertos informáticos anti-éticos para conseguir información de aquellos que sufren

estos ataques cibernéticos, los cuales están basados la creatividad de los *hackers* o *crackers* de aprovecharse de fallas de seguridad y hacerse pasar por entidades u organizaciones fidedignas o sitios web debidamente verificados. Los ataques basados en ingeniería social se aprovechan de las imperfecciones de la mente y en el comportamiento del ser humando, puesto que pueden aprovecharse de la ignorancia o falta de conocimiento en el manejo de un ordenador sin tomar las medidas correspondientes para no exponerse a ataques informáticos, tomando en cuenta aspectos psicológicos y patrones de conducta para poder formas estas artimañas para ser cada vez más precisos. (Romano Ozcáriz, 2019, p. 127-128)

Como podemos observar, aunque estos delitos dependan del uso de un sistema informático, siempre se debe tener en cuenta la capacidad de la mente humana para utilizar estas herramientas en ilícitos, y que sin su participación dichas tecnologías no serían más que un montón de artilugios y aparatos sin vida. Por esto es importante un tratamiento normativo que pueda identificar a los causantes de estos delitos, ya que sin esto no se puede sancionar a sus autores ni reunir los elementos necesarios para considerarlo como una conducta penalmente relevante para el ordenamiento.

1.5. El *Ransomware* como Delito Informático en el Ecuador

1.5.1. Definiciones y Concepto de *Ransomware*

El término *Ransomware* en su traducción literal se puede definir como un *software* o programa de secuestro de datos. Estos *malwares* o *softwares* maliciosos creados y controlados por los sujetos autores del delito se encargan de encriptar, ocultar o de retener información y datos dentro de un ordenador o servidor, con el afán de solicitar una recompensa o monto económico por la liberación de los archivos

encriptados, tal y como se describe la naturaleza de un delito de secuestro de personas. Este ataque informático se especializa en infectar a toda clase de sistema operativo, es decir tanto Windows, Linux, Ubuntu, macOS, entre otros más. Sin embargo, existen sistemas operativos más propensos a verse afectados por estos softwares maliciosos, siendo Windows el más perjudicado al igual que dispositivos que funcionen este sistema o aquellos con un sistema Android, esto debido a la facilidad que existe en su programación para la distribución de código malicioso. (Estrada Cola, 2018)

Se conoce por *ransomware* al malware o software malicioso que opera en el ordenador en el que se haya inmiscuido apoderándose de la información contenida en él y tomando control del acceso que tiene el usuario a ella, generalmente solicitando un pago como rescate de la información cifrada; en esta clase de conducta el autor del secuestro es el único que tiene conocimiento de la contraseña del cifrado, por lo que la víctima queda a total merced de su voluntad debiendo hacer lo que se le solicite si es de su deseo el obtener esta contraseña. Esta conducta tiende a evolucionar por varios factores, entre ellos la ingeniería social y las fallas detectadas por los piratas informáticos para valerse de ellas. (Trigo et al., 2017)

Por otro lado, el *Ransomware* llega a ser definido por Barker et al. (2022) como un *software malicioso* creado con el fin de cifrar o encriptar información de instituciones y organizaciones, centrándose únicamente en la información de entidades y de empresas, con ello logrando acorralar a los directores de las mismas exigiéndoles una compensación económica como rescate por el desencriptado de los datos secuestrados y por la no divulgación de los mismos, ya que esto puede ser perjudicial

para la privacidad de sus usuarios y del funcionamiento de las empresas afectadas en el supuesto de darse. (p. 2)

Tras haber analizado el concepto del *ransomware* como un *malware* creado con la finalidad del cifrado de datos y coincidiendo los autores citados anteriormente con este criterio, es pertinente señalar que además de tratarse de un simple *software* el *ransomware* llega a ser el término acuñado en Derecho para la conducta a través de la cual un experto informático encripta información de un ordenador atacado con este virus, no limitándose así únicamente su uso para el nombre del *malware*. Es importante señalar esta característica, debido a que algunos trabajos de investigación definen al *ransomware* como un elemento de otras conductas ya existentes dentro de las legislaciones, lo cual va en contra de la finalidad del Derecho Penal Informático de servir como un complemento para el Derecho Penal General para la debida regulación de los Delitos Informáticos.

1.5.2. Población vulnerable a los ataques *Ransomware*

Como bien conocemos, dentro de los Delitos Informáticos cualquier persona con un ordenador o dispositivo inteligente con acceso a internet puede llegar a ser víctima de un ciberdelito ya que no existe un protocolo totalmente seguro para su prevención, llegando a ser impredecible el momento o la situación bajo la cual nosotros mismo seamos objeto de dichos ilícitos. Empero, el *Ransomware* doctrinariamente está caracterizado porque afecta en su totalidad al bien jurídico de los delitos jurídicos por excelencia, definido a su momento como la Funcionalidad Informática o la utilidad que posee la información contenida en los sistemas informáticos para su dueño puesto que puede ser vital para el libre desarrollo de su persona dentro de la sociedad.

Por lo general el blanco de los ataques de secuestro de datos suelen ser aquellas empresas u organizaciones con información que, por su naturaleza, es imprescindible que deba ser protegida y no divulgada porque constituyen datos de valor para la empresa y para los usuarios y que, en el caso de ser distribuida, esto significaría un peligro para la integridad de la empresa y de sus clientes; pueden ser empresas privadas, estatales, de beneficencia, o de cualquier tipo en la que se ponga en juego bases de datos o acciones que se encuentren digitalizadas o almacenadas en servidores y ordenadores. (Barker et al., 2022)

1.5.3. Tipos de Ransomware

Al respecto Moreno et al. (2020) señalan que los *ransomware* se clasifican de diversas formas: por su comportamiento, el cual bloquea el acceso al sistema operativo, a su vez cifra archivos y datos del sistema operativo infectado. Igualmente, según su tecnología podemos clasificarlos de la siguiente manera:

- *FAKEAV*: sirven como método de engaño para los usuarios que buscan comprar antivirus especializados en malware, por medio del uso de ingeniería social y de publicidad engañosa.
- *Ransomware* de compresión: sirven para reunir varios archivos y comprimirlos en el ordenador en una carpeta comprimida (generalmente formato ZIP), dentro de la cual el extorsionador coloca un aviso con las instrucciones para poder entregar la contraseña de desbloqueo de los archivos.

- *SMS Ransomware:* son mensajes enviados con la finalidad de que la víctima concluya con el pago del secuestro. Por lo general son usados como complementos en ataques de secuestro de datos
- *Ransomware* desarrollados para inferir en el proceso de iniciación del sistema operativo del sistema informático atacado, impidiendo esta acción y colocando un aviso de rescate al encender el ordenador, en el que asevera la obligación de efectuar el pago para la liberación de su equipo.
- *Police Ransomware:* es utilizado como método de engaño, en el que las víctimas son extorsionadas por la supuesta comisión de actividades ilícitas, solicitando los piratas informáticos un pago por la eliminación de dichos cargos falsos y para no continuar con el proceso legal. (pp. 1-2)

Los diversos tipos de *ransomware* y su modalidad están determinados netamente por la ingeniería social, creándose así cada uno dependiendo del tipo de engaño que se quiera emplear, tal y como hemos analizado. En este punto podemos resaltar la importancia de la mente humana en estos delitos y reafirmando el punto de que sin el ingenio humano estos sistemas informáticos son simples artilugios sin funciones.

1.5.4. Modos de Difusión del *Ransomware*

Este secuestro de datos además de ser realizado a voluntad de los *hackers* o *crackers* para obtener un beneficio directo del rescato de datos también puede ser contratado por otra persona como un servicio a través del cual puede hacerse de datos o información de otra persona u organización que pueda ser de su utilidad. Es por este particular que los ciberdelincuentes han optado por revolucionar mucho más las formas

por las cuales pueden propagar estos malwares e invadir ordenadores con mayor efectividad, ofreciendo así un trabajo certero y confiable a quienes lo requieran.

Moreno et al. (2020) al respecto analizan como modos de propagación de este malware a diversos escenarios creados por los mismos piratas informáticos, tal y como lo es: la redirección a sitios web infectados desde *ads* publicitarios colocados en otras páginas populares o mayormente visitadas por los internautas; correos electrónicos que aparentan ser de entidades o empresas en los que el usuario abre links que implantan los *malware ransomware* en el ordenador desde el navegador web; el uso de *botnets* o mayormente conocidos *bots informático*, que están programados para inmiscuirse en el sistema a infectarse de una forma genuina, es decir sin códigos maliciosos, para que inmediatamente se instalen los *malwares* con código malicioso sin que la víctima tenga conocimiento de este hecho sino hasta el momento en el que se le notifica del secuestro; la ingeniería social o técnicas de engaño de los *hackers* para crear situaciones de vulnerabilidad en la seguridad de los ordenadores de las víctimas; y por último la contratación de servicios de *Ransomware* señalada en párrafos anteriores, que a su vez es un método de propagación de todos los otros métodos señalados, ya que en ella para obtener el resultado deseado el experto puede emplear un modo de propagación o, de ser necesario, más de uno, dependiendo de lo solicitado por su cliente. (p. 4)

1.5.5. Instrumentos Internacionales y legislación comparada sobre Delitos Informáticos y *Ransomware*

Los Delitos Informáticos y el Ransomware han sido objeto de estudio por parte de varios ordenamientos jurídicos y por parte del mismo Derecho Internacional, puesto

que han significado una complicación en la seguridad y la privacidad de los países afectados y de las personas que pertenecen a ellos, y al no ser capaz el Derecho de poder crear métodos para determinar con exactitud sobre quien recae la responsabilidad penal de estos hechos se ve en la tarea de realizar convenciones en la que se convoque a aquellos Estados con preocupación por el tratamiento del *Ransomware* para poder regular estas situaciones.

El Convenio de Budapest creado por el Consejo de Europa (2004) es considerado como el instrumento internacional que fue un precursor en la creación de regulaciones de Delitos Informáticos o Ciberdelitos, ofreciendo por primera vez el concepto del delito informático como una conducta cometida por medio de la web o por con el uso de sistemas informáticos como principal herramienta para su conclusión. Además, desplegaba conceptos, definiciones, ámbitos de aplicación, procedimientos y formas unificadas de proceder ante estos delitos, además de otorgar un catálogo de delitos relativamente nuevo para la fecha de su creación, tipificándose entre ellos los delitos de reproducción de pornografía infantil, delitos contra la propiedad intelectual, fraudes informáticos y demás delitos informáticos que según los treinta Estados contratantes y los dieciséis adherentes son los más cometidos dentro de sus jurisdicciones y que urgen un pronto tratamiento de acorde al contexto social de cada uno.

No existe como tal una regulación específica dentro de tratados o instrumentos internacionales sobre delitos informáticos para lo que se conoce como *Ransomware*, debido a que es una conducta nueva en comparación con los tratados creados en su momento. Sin embargo, si bien el Derecho Internacional no ha tratado directamente

esta problemática, existen Estados que independientemente de ello ha creado regulaciones y medidas de prevención y de mitigación de daños proferidos por ataques *Ransomware*, tal y como lo son los casos de las siguientes legislaciones a analizarse:

a) Legislación Española

El Gobierno español ha considerado la necesidad de adoptar una regulación en contra del *Ransonware* considerando que ya no se trata de un simple cifrado de datos, o de un robo de información que se da comúnmente entre sistemas informáticos; esto debido a que sus autoridades y legisladores han determinado como meollo del asunto a regular el obtener una retribución económica a cambio de causarle daño a otra persona.

El Centro Criptológico Nacional (2016) desprende una regulación en el año 2018 denominada “Medidas de seguridad contra *ransomware* CCN-CERT IA-11/18”, dentro de la cual establece los parámetros básicos a tomarse en cuenta para la prevención, tratamiento y procedimientos legales a seguirse frente a ataques de secuestro de datos. Dentro de este reglamento se encuentran desde antecedentes históricos del *ransomware*, definiciones, las vías de infección por las que se propaga, además de contener un catálogo de los malwares ransomware detectados en el territorio español que han sido tratados en mayor cantidad de ocasiones, de los cuales podemos destacar los virus *WannaCry*, *Crysis*, *Cerber*, *Locky*, y *NotPetya*, variantes que además de afectar a la población española causaron estragos alrededor de todo el mundo. Adicionalmente de brindar estas medidas preventivas e información sobre dichos ataques, este reglamento ofrece una serie de medidas que se podrían adoptar para el desencriptado o la recuperación de la información que ha sido secuestrada, al igual que

un listado que contempla la posibilidad de recuperación de la información frente a determinadas variantes de *ransomware*, educando así a la gente a hacer frente a estos ataques desde la prevención hasta la mitigación o reparación de los daños causados a los datos, a pesar de que es una conducta que no puede ser anticipada fácilmente.

b) Legislación Peruana

La legislación penal en Perú ha adoptado otro rumbo para poder enfrentar al *ransomware* como una conducta que afecta en tiempo real a la población, ya que a diferencia de España que creó una normativa centrada únicamente en la regulación de este fenómeno, en el ordenamiento jurídico peruano se adecúa al secuestro de datos dentro de otro tipo penal ya existente, que protege efectivamente la Funcionalidad Informática como el bien jurídico protegido en este delito.

El Congreso de la República (2013) dentro de la Ley de Delitos Informáticos/Ley N° 30096, en su artículo 4 establece lo siguiente:

Artículo 4.- Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. (p.2)

Dentro de este artículo podemos analizar que se comprende como sujeto activo a una persona con cierta pericia dentro de la Informática y Sistemas, ya que la conducta debe realizarse estrictamente por medio del uso de sistemas informáticos; como sujeto pasivo o víctima a aquella persona que se ve afectada en la integridad de

los sistemas informáticos de su pertenencia o de empresas a las que pertenezca; como conductas como bien jurídico tenemos la funcionalidad de los sistemas informáticos que se ve afectada por el secuestro; como conductas punibles el inutilizar total o parcial los sistemas, impedir el acceso a estos, y por último el alterar temporal o permanentemente los servicios brindados por medios de estos sistemas. Con este análisis podemos notar que se enmarca con los presupuestos descritos en la conducta de Secuestro de Datos o *Ransomware*, pero no se regulan aspectos como la extorsión que es efectuada de dicho secuestro de información.

En conclusión, el ordenamiento jurídico peruano a diferencia del español adoptó dentro de su ordenamiento una Ley dedicada específicamente al tratamiento de Delitos Informáticos; no obstante, no descuidó aspectos como la protección de la Funcionalidad Informática como bien jurídico protegido en estos delitos, bien que por lo general resulta verse menoscabado en casi todos los delitos informáticos al ser la información el objetivo principal de sabotaje, siendo ese el caso del *Ransomware* al adecuarse al presupuesto planteado en el artículo 4 de dicha Ley y siendo sancionado debidamente con la pena establecida.

Tras haber establecido los conceptos básicos, modalidad y tipos de *ransomware*, me permito agregar a manera de síntesis lo siguiente: el *ransomware* es un *software malicioso* creado en base a código malicioso que se encarga del encriptado de información del ordenador o sistema dentro del cual fue implantado, con lo cual se envía un mensaje a la víctima del encriptado de datos anticipando un pago al delincuente informático como intercambio por la liberación de la información, bajo el riesgo de que dicha información no sea liberada ni aun así efectuando el pago; existen

varias clases *ransomware*, cada una diferenciándose de la otra de acuerdo a la modalidad y el alcance del encriptado que poseen; además de que estos malwares son distribuidos con la intervención de personas que hacen uso de ingeniería social (métodos de engaño basados en aprovecharse de víctimas con poco o carente conocimiento en informática básica); y por último, contemplamos que legislaciones como la española o la peruana, que es más próxima a nuestra realidad, poseen una regulación para este tipo de conductas, ofreciendo así en sus normativas desde conceptos básicos hasta sanciones y métodos de mitigación de los daños producidos en los ordenadores objeto de este secuestro, lo cual implica que un debido tratamiento del *ransomware* en nuestra realidad debe involucrar todos estos aspectos que según el derecho comparado son necesarios para normar este nuevo fenómeno que se ha dado lugar en los últimos años.

2. Capítulo II: Análisis para identificar los Delitos Informáticos tipificados en el Código Orgánico Integral Penal

Tras haber establecido el concepto y definición de lo que llega a ser un delito informático desde un punto de vista doctrinario y teniendo clara su naturaleza jurídica, es importante analizar el ordenamiento jurídico ecuatoriano con el fin de determinar si nuestros legisladores han puesto empeño en crear una regulación sobre delitos informáticos, y de ser el caso, desglosar los elementos de cada tipo penal para poder satisfacer la interrogante planteada al inicio de esta investigación y poder determinar con precisión si existe o no regulación aplicable al *ransomware*.

Dentro de nuestra normativa se encuentra vigente el Código Orgánico Integral Penal desde el año 2014, el cual nos ofrece un catálogo de delitos informáticos que

llega a encontrarse disperso dentro de su contenido tratando de abarcar nuevas conductas relacionadas con la difusión o reproducción de contenido pornográfico, delitos contra la propiedad intelectual y derechos de autor, falsificaciones y estafas informáticas, entre otros delitos relacionados con el uso de tecnología.

Si bien tenemos claro que dentro de dicho Código sí existe una regulación pertinente a delitos informáticos, es fundamental que se emplee un análisis gramatical jurídico de todos los tipos penales relacionados a estos delitos para determinar si en alguno de estos tipos se sanciona la conducta del *ransomware* o si alguna figura se asemeja a su modo de comisión para su sanción. Al respecto Ortiz Campos (2019) añade lo siguiente:

> Las áreas de estudios establecidas por Bolaños y Gómez (2015) con sus respectivos artículos son: 1) violación a los derechos humanos, diversas formas de explotación articulo 103; 2) delitos contra el derecho a la intimidad personal y familiar artículos 178,179 y 180; 3) delitos contra el derecho al honor y buen nombre articulo 182; 4) delitos contra el derecho a la propiedad artículos 190,191,192,193,194 y 195; 5) delitos contra el derecho a la integridad articulo 298; (…) 7) delitos contra la seguridad de los activos, sistemas de información y comunicación artículos 229,230,231,232,233 y 234(…). (p. 104)

En el presente capítulo se efectuará un análisis gramatical jurídico de los tipos penales mencionados en la cita previa, consistente en el desglose de los elementos que constituyen el tipo penal, desde los sujetos que intervienen en él, siendo sujeto activo (calificado o no calificado), sujeto pasivo, conducta punible, verbo rector, entre

otros elementos que son propios de los tipos penales en su regulación para que puedan tener efectividad.

2.1. Análisis Doctrinario del Tipo Penal

Antes de realizar el análisis de los tipos penales creados para la regulación de los delitos informáticos en la normativa penal de nuestro ordenamiento, se debe realizar una revisión conceptual y doctrinaria de lo que es el tipo penal y de sus elementos, tanto objetivos como subjetivos, para poder establecer los aspectos fundamentales de la Tipicidad dentro de la Teoría del Delito, fijando así los requisitos del análisis a realizarse posteriormente en la presente investigación.

Es sustancial establecer la diferencia de significados que existe entre la Tipicidad y el tipo penal, puesto que, si bien aparentan ser figuras semejantes acarrean una diferencia importante que hace que una figura sea parte de la otra y se complementen mutuamente en la Teoría del Delito, siendo esta el área que busca estudiar la conducta del ser humano en cuanto a una adecuación a un delito descrito en la normativa penal. El tipo penal por una parte puede ser definido como aquella creación normativa por parte de legislador mediante la cual describe los detalles necesarios para que un hecho que cumpla con ellos sea encuadrado por un delito y los plasma en la ley penal correspondiente; dicho de otra manera, el tipo penal hace alusión a la tipificación de un hecho catalogado como delito con sus presupuestos descritos, que al encuadrarse con la realidad acarrean responsabilidad penal a quien o quienes lo hubieran cometido. Por otra parte, la Tipicidad ha sido definida por la doctrina como aquel acto que realiza el jurista, juez, fiscal, entre otros profesionales del Derecho, para encuadrar una conducta cometida que se asemeje a los presupuestos

descritos en la normativa penal, es decir en el tipo penal, para así sancionar el ilícito debidamente. (Echeverría et al., 2019, pp. 332-333)

Fijada esta línea, el tipo penal llega a ser definido como aquella descripción que efectúa el legislador de aquellas conductas que llegan a ser consideradas como delitos dentro del ordenamiento jurídico, y que acarrean responsabilidad penal sobre la persona o grupo de personas que llegasen a ser determinados como autores de dichas conductas contrarias al orden jurídico.

Echeverría et al. (2019) aclara que el tipo penal llega a tomar mayor relevancia en la teoría del delito al darse el acto de tipicidad sobre un hecho que se quiere determinar como un delito, ya que mediante la operación de tipicidad el tipo penal llega a ser encuadrado a un caso en concreto y se genera una pena inmediata hacia el agente al momento en el que se convierte en un delito, dándole así sentido a su creación. Además, concuerda con otros autores en que los elementos básicos del tipo penal son tres: los sujetos, el bien jurídico protegido y la acción. (p. 333) Para el análisis a efectuarse se utilizará como referencia de los elementos básicos del tipo penal el criterio del jurista Echeverría en cuanto a los sujetos, bien jurídico protegido, y la acción, además de incluir a la pena que se establece en los tipos, que a mi parecer complementa mucho más este ensayo.

2.2. Análisis del Tipo Penal de los Delitos Informáticos del Código Orgánico Integral Penal

Los artículos a analizarse forman parte del Código Orgánico Integral Penal aprobado por la Asamblea Nacional de la República del Ecuador (2014) y publicado en el Registro Oficial No. 180, vigente en la actualidad. Además, los bienes jurídicos

protegidos a analizarse forman parte del contenido del mismo código y de los Derechos consagrados en el artículo 66 de la Constitución de la República del Ecuador aprobada por la Asamblea Nacional Constituyente (2008):

> ***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.*
>
> *Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.*
>
> *Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo I, Sección Tercera, Art. 103***. Registro Oficial.)

Dentro de este artículo en su primer inciso se identifica como sujeto activo a una persona no calificada; el sujeto pasivo, o en este caso sujetos pasivos, llegan a ser niños, niñas y adolescentes, que a su vez forman parte de un grupo de atención prioritaria dentro de la Constitución de la República; como bien jurídico protegido se determina el Derecho Humano a la integridad sexual de los menores; y como verbos rectores de la conducta punible serían “fotografiar”, “filmar”, “grabar”, “producir”, “transmitir” o “editar” cualquier clase de material audiovisual que contenga imágenes de menores de edad cometiendo actos de naturaleza sexual, sin importar que el origen del video sea del territorio nacional o en el extranjero, y conducta que es sancionada con

una pena privativa de la liberta de trece a diecinueve años; en el segundo inciso se hace alusión al caso de poseer el menor o menores enfermedades catastróficas o graves, o discapacidad, esta pena aumenta de dieciséis a diecinueve años; y adicionalmente en el último inciso contempla la situación en la que el sujeto activo fuese cualquier familiar o pariente hasta el cuarto grado de consanguinidad y segundo de afinidad, o tutor, profesor, o cualquier persona que ejerciendo una profesión o actividad abuse de ello para abusar de niños, niñas o adolescentes se sancionará con una pena privativa de la libertad de veintidós a veintiséis años; el condicionante de este delito es que la divulgación o cualquier acción realizada con el material pornográfico generado sea realizado contra niños, niñas o adolescentes, y que a su vez sea perpetrado por parientes o personas cercanas a las víctimas en razón del uso de su autoridad como tutor, profesor, o cualquier otra situación de poder frente a las víctimas, o en su defecto el valerse de discapacidades o enfermedades de las víctimas para cometer este ilícito.

Tomando en cuenta los elementos enunciados sobre los delitos informáticos, en cuanto a su forma de comisión a través de sistemas informáticos hacia otros sistemas, este tipo no se ajusta a la forma de comisión de la conducta de *ransomware* ni pretende regular delitos informáticos que afectan a la integridad y funcionamiento de los sistemas como tal, siendo este el bien jurídico a tutelarse la funcionalidad informática, y no como en el presente caso que se tiene como bien jurídico protegido la integridad sexual de los menores de edad.

> ***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.*
>
> *No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Sexta, Art. 178***. Registro Oficial.)

En este tipo penal se puede determinar al sujeto activo como no calificado, pudiendo llegar a ser cualquier persona que actúe sin el consentimiento o autorización legal de la otra parte; como sujeto pasivo a la persona que es objeto de la violación a su intimidad; el bien jurídico protegido en este tipo es el Derecho a la intimidad personal y familiar; como verbos rectores podemos encontrar el "acceder", "interceptar", "examinar", "retener", "grabar", "reproducir", "difundir", y "publicar" cualquier clase de información, incluyendo mensajes, audios, fotografías, videos, o cualquier material que pueda ser difundido por medios tecnológicos o de comunicación; y sancionando esta conducta con una pena privativa de la libertad de uno a tres años, excluyendo los casos en los que en dicha información o datos forma parte la persona que los reproduce, o aquella información que es catalogada como pública; el condicionante en este supuesto llega a ser la voluntad y el consentimiento expreso de la persona a quien pertenece los datos y de quien se violenta la intimidad al momento de consentir el manejo de sus datos, caso contrario de no poseerlo se recae en esta conducta típica.

En el presente tipo, si bien se hace referencia a la utilización de medios tecnológicos, y hasta de ordenadores, el alcance de este artículo no regula el secuestro de datos o *ransomware* en nuestra legislación penal, ya que en este caso se regula la

reproducción o difusión de material de índole personal sin consentimiento, mas no el secuestro de datos ni se tiende a proteger la funcionalidad informática.

> ***Art. 179***.- ***Revelación de secreto o información personal de terceros***. - *La persona que teniendo conocimiento por razón de 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.*
>
> *Será sancionada con pena privativa de libertad de uno a tres años quien revele o divulgue a terceros contenidos digitales, mensajes, correos, imágenes, audios o vídeos o cualquier otro contenido íntimo de carácter sexual de una persona en contra de su voluntad.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Sexta, Art. 179***. Registro Oficial.)

El sujeto activo en este tipo penal llega a ser calificado, siendo aquella persona que se valiese de su estado o vínculo personal frente a la víctima, o de su profesión, oficio, trabajo, puesto, o situación análoga cometa dicha conducta; el sujeto pasivo es la persona o grupo de personas a los que pertenece la información o secreto; el bien jurídico protegido es el Derecho a la intimidad personal y familiar rectores de esta conducta son el “divulgar” y “revelar” dicho secreto o información íntima; con una sanción que contempla una pena privativa de la libertad de seis meses a un año, exceptuando aquellos casos en que la información que se revele tenga relación con hechos de conocimiento público. El último inciso, que es el de nuestro interés, prevé la situación en la que esta divulgación se dé mediante medios digitales como fotos, correos electrónicos de contenido sexual de la víctima sin su consentimiento, dándose por medio del uso de tecnologías; el condicionante del delito en este caso es la posición de poder en la que se encuentra el sujeto activo frente al pasivo y de la que se

vale para realizar la conducta, y de la consciencia que tiene el sujeto pasivo del daño que cause esta revelación de información.

Para este artículo, haremos un breve análisis del segundo inciso que trata sobre el uso de tecnologías para el cometimiento del ilícito. El tipo penal sanciona la divulgación de contenido de este tipo con la utilización de medios digitales, que, si bien se dan lugar las nuevas tecnologías y los sistemas, en esta situación no se produce el secuestro de datos de ningún tipo y el bien jurídico protegido no es la funcionalidad de sistemas informáticos, sino la intimidad y la privacidad del sujeto pasivo, por lo que el presente tipo penal no regula el *ransomware* o secuestro de datos.

> *Art. 180.-* ***Difusión de información de circulación restringida. -*** *La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años*
> *Es información de circulación restringida:*
> 1. *La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.*
> 2. *La información producida por la Fiscalía en el marco de una investigación previa.*
> 3. *La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Sexta, Art. 180*.** Registro Oficial.)

El sujeto activo en este tipo no es un sujeto calificado; el sujeto pasivo en el presente caso es la sociedad en general puesto que puede ser cometido contra cualquier persona; el bien jurídico protegido es el Derecho a la intimidad personal y familiar; el verbo rector es “difundir” dicha información restringida; la sanción en este delito es una pena privativa de libertad de uno a tres años; el condicionante viene a ser el sujeto pasivo tiene que difundir información catalogada estrictamente como

restringida, entendiéndose por “información de circulación restringida” la que por su naturaleza o que por cualquier cláusula celebrada se le haya otorgado el carácter de confidencial o de acceso restringido para todo el público, la que es producida por parte de Fiscalía en los periodos de investigación previa, y aquella de la que son titulares niños, niñas y/o adolescentes en la que su divulgación significaría una grave violación a los derechos de los menores al tenor del Código Orgánico de la Niñez y la Adolescencia.

Este tipo penal por sus elementos y conducta que sanciona no cubre con la regulación ni sanción del secuestro de datos o *ransomware*, ni tiene como bien jurídico la funcionalidad informática; por otra parte, esta tipificación involucra a los sistemas informáticos en el proceso de obtención de dicha información y en su divulgación, pero no así en el proceso de afectar a otro sistema ni del encriptado de esta información mencionada, por lo que no sanciona la conducta estudiada.

> *Art. 182.-* ***Calumnia. -*** *La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.*
>
> *No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.*
>
> *No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.*
>
> *No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad.* (Tomado

de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Séptima, Art. 182***. Registro Oficial.)

El sujeto activo en el presente artículo no es un sujeto calificado, pudiendo ser perpetrado por cualquier persona; el sujeto activo es la persona sobre la que verse esta calumnia o falsa imputación; el bien jurídico protegido es el Derecho al honor y al buen nombre; el verbo rector es el “realizar” dicha imputación falsa; la sanción impuesta es una pena privativa de la libertad de seis meses a dos años; además, se hace referencia a dos casos en particular en los que no se constituye calumnia: cuando las aseveraciones se hagan frente a autoridad competente, y cuando estas se llegasen a comprobar, y al caso en el que el sujeto activo se retractase de las calumnias proferidas varias veces por los mismos medios por los que las cometió no se acarreará responsabilidad penal; el condicionante de este tipo penal es que las aseveraciones que se realizan sobre el sujeto pasivo no vayan de acorde a la realidad y que carezcan de veracidad o pruebas.

El análisis principal de este tipo recae en la utilización que se da de medios tecnológicos y sistemas informáticos para su comisión. Las calumnias se puedan dar lugar mediante el uso de ordenadores o varios medios tecnológicos. Empero, si tenemos en cuenta la naturaleza planteada en la investigación sobre los delitos informáticos, esta conducta no se categoriza como uno de ellos, ya que no afecta a la funcionalidad informática de los aparatos empleados, ni se da el secuestro de información de ningún tipo. En conclusión, este tipo penal no regula de forma alguna *ransomware* o cualquier delito informático.

> *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 transferencia 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 secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 190****.* Registro Oficial.)

En este delito el sujeto activo no es un sujeto calificado; el sujeto pasivo es la persona titular de los bienes, valores o derechos objeto de apropiación; los verbos rectores son “utilizar”, “facilitar”; el bien jurídico protegido es el Derecho a la propiedad; la pena que se determina es una privación de la libertad de uno a tres años; el condicionante de este tipo penal es que dicha apropiación sea efectuada de forma ilegítima y no consentida por el titular de dichos derechos, o que en su defecto se busque hacer daño a terceras personas mediante la apropiación de información del sujeto pasivo principal, adicionalmente contemplando la situación de dicha apropiación si se comete mediante el sabotaje o inactivación de sistemas de seguridad.

Este delito no puede catalogarse como Delito Informático, ya que no se afecta a la funcionalidad de ningún sistema empleado para la apropiación fraudulenta, sino por otra parte se utiliza el sistema como un medio para obtener de forma ilegal dichos títulos del sujeto pasivo. Así logramos determinar que este artículo no cumple con los presupuestos para regular la conducta del secuestro de datos o *ransomware.*

> *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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 191****.* Registro Oficial.)

En el presente artículo el sujeto activo no es un sujeto calificado, por lo cualquier persona podría efectuarlo; el sujeto pasivo es la sociedad en general; el bien jurídico protegido es el Derecho a la propiedad; la pena impuesta en este artículo es una pena privativa de la libertad de uno a tres años; el condicionante en esta conducta es la alteración de la información verificada por el Estado en su organismo de control correspondiente de los equipos terminales móviles.

El presente tipo penal no tiende a regular delitos informáticos o algún hecho que afecte a la funcionalidad de los sistemas informáticos, sino por otro lado afecta el control que posee del Ministerio de Telecomunicaciones sobre los terminales móviles y su origen (datos de serie, homologación del dispositivo, etc.). Con este fundamento se determina que este artículo no regula la conducta objeto de la presente investigación.

> *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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 192****.* Registro Oficial.)

El sujeto activo en este delito no es calificado; el sujeto pasivo es la sociedad en general puesto que cualquier individuo puede resultar como víctima de este hecho; el bien jurídico protegido es el Derecho a la propiedad; los verbos rectores se identifican como el “intercambiar”, “comercializar” y comprar” dichas bases de datos con

información de equipos terminales móviles; la sanción impuesta es de una pena privativa de la libertad de uno a tres años; el condicionante llega a ser el intercambio económico que se produce por la obtención de la información de bases de datos relacionada con equipos terminales móviles.

Dada la situación, por los elementos de este tipo penal y la conducta que regula se puede determinar que no es un delito que se realiza por medio de sistemas informáticos en contra de la integridad de otros sistemas semejantes, es decir no es un delito informático dentro del margen de esta investigación, y además no atenta contra la funcionalidad de estos sistemas ni encripta información contenida en ellos, por ende, este tipo no regula el *ransomware.*

> *Art. 193.-* ***Reemplazo de identificación de terminales móviles.-*** *La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 193***. Registro Oficial.)

El sujeto activo en este tipo penal no es calificado, puesto que no depende de ningún factor, oficio, trabajo, u puesto para su comisión; el sujeto pasivo es la sociedad en general; el bien jurídico protegido es el Derecho a la propiedad; el verbo recto es el de “reemplazar” dichas etiquetas de fabricación de los equipos terminales móviles por etiquetas falsas; la sanción impuesta en este tipo penal recae en una pena privativa de la libertad de uno a tres años; el condicionante en el presente caso es el reemplazamiento y eliminación total de la información original de los equipos terminales móviles.

Mediante el análisis gramatical del presente artículo es claro que no involucra el uso de sistemas informáticos en contra de otros en su integridad o funcionamiento, sino que versa sobre la falsificación de la información de origen de los equipos objeto del delito. Con este fundamento notamos que este tipo no regula el secuestro de datos o *ransomware*.

> *Art. 194.-* ***Comercialización ilícita de terminales móviles.-*** *La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 194.*** Registro Oficial.)

El sujeto activo en el presente delito tipificado no es un sujeto calificado; el sujeto pasivo es la sociedad en general al verse afectada por la comercialización ilícita de móviles; el bien jurídico protegido es el Derecho a la propiedad; se impone una pena privativa de la libertad de uno a tres años para el autor o autores del ilícito; el condicionante en esta conducta es la comercialización de equipos terminales móviles que violen los procedimientos y requisitos impuestos por el Estado en su órgano de control respectivo para operar normalmente dentro del territorio.

En esta tipificación podemos notar que se pone en riesgo el orden económico y las normas impuestas para la comercialización de los móviles, además de violentar el derecho a la propiedad en el caso que las terminales móviles se hayan obtenido mediante sustracción involuntario del mismo a su anterior dueño. Al poseer estos elementos y al regular la conducta analizada, es pertinente aseverar que este artículo no tiende a regular delitos informáticos, ni mucho menos el *ransomware* o encriptado de información de sistemas informáticos.

> *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.*
> *No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo II, Sección Novena, Art. 195****.* Registro Oficial.)

El sujeto activo no resulta ser calificado en este delito; el sujeto pasivo llega a ser la sociedad en general; el bien jurídico protegido en esta conducta es el Derecho a la propiedad; la pena impuesta es la privación de la libertad de uno a tres años para quien lo hubiese cometido; el condicionante viene a ser la posesión como tal de cualquier mecanismo electrónico o digital empleado con el fin de la alteración de la información de identificación de los equipos terminales móviles, excluyendo los programas para apertura de bandas como objeto del delito.

Como podemos observar, el presente artículo no busca la regulación del *ransomware*¸ sino por otro lado busca el regular y evitar la modificación de la información de serie de dispositivos móviles, campo de acción que no es del interés de la presente investigación.

> *Art. 229.-* ***Revelación ilegal de base de datos.-*** *La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.*
>
> *Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.* (Tomado de Asamblea

Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 229***. Registro Oficial.)

En el supuesto del primer inciso de este artículo el sujeto activo no es calificado, el sujeto pasivo llega a ser la persona o grupo de personas a las cuales pertenecen los datos pertenecientes a dichas bases; el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena impuesta en este inciso es una de uno a tres años de privación de la libertad; el condicionante en este delito es la consciencia y la voluntad con la que actúa el sujeto pasivo al momento de cometer la revelación de dicha información

Por otro lado, el segundo inciso del mismo tipo contempla un sujeto activo calificado, ya sean servidores públicos, empleados bancarios internos o de las instituciones descritas; además se impone una pena privativa de la libertad de tres a cinco años.

En esta conducta el uso de sistemas electrónicos e informáticos llega a ser más concurrido puesto que en la actualidad las bases de daros se almacenan en dispositivos electrónicos o en nubes digitales de información y se adecúa al presupuesto planteado en la investigación sobre la modalidad de comisión de un delito estrictamente informático. Sin embargo, si bien se accede a estas bases de datos en medios digitales para la revelación de su contenido el sujeto activo no solicita una retribución económica para hacerlo, y mucho menos realiza una encriptación de la información con el fin de causar mal a quienes poseen titularidad sobre la información, no adecuándose así a la modalidad del *ransomware* ni regulando este artículo la conducta mencionada.

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. (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal, *Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 230***. Registro Oficial.)

El presente artículo regula la interceptación ilegal de datos en cinco numerales que regulan diferentes supuestos basados en la misma conducta. El sujeto activo en los supuestos no es calificado; los sujetos pasivos llegan a ser las personas titulares de la información que fue interceptada; el bien jurídico protegido llega a ser la Seguridad de los Activos de los sistemas de Información y Comunicación; los verbos rectores son

“interceptar, “escuchar”, “desviar”, “grabar”, “observar”, “desarrollar”, “ejecutar”, “producir”, “programar”, “enviar”, “poseer”, “vender”, “distribuir”; “introducir”, “copiar”, “clonar”, “comercializar”, “producir”, “fabricar”, “distribuir”, “poseer”, “facilitar”; la pena impuesta es de la privación de la libertad de tres a cinco años; el condicionante se basa en el carácter ilegal de esta interceptación de datos o de cualquier actividad que esté destinada a alcanzar como fin esta conducta ya señalada. En tal modo, la ilegalidad del fin y de los medios utilizados para la interceptación es el condicionante de este tipo penal.

Este artículo abarca varios elementos que se asemejan a la conducta del *ransomware*, como lo es el crear un escenario en el que la víctima voluntariamente acceda a sitios web o instale en su equipo programas o herramientas que faciliten la interceptación de la información para poder infiltrarse dentro del equipo u ordenador de quien sea víctima de este hecho. De igual manera, hace referencia a la apropiación no consentida de estos datos por parte del sujeto activo con la utilización de un sistema electrónico o informático, la cual se da con el fin de perjudicar a los titulares. Sin embargo, si bien este tipo penal se asemeja a una regulación para el *ransomware* **no** está facultado para sancionarlo, puesto que se toma como bien jurídico protegido únicamente a los datos infiltrados y no a la funcionalidad de los sistemas que se ven violentados para la interceptación de las bases de datos, y además no se toma como modalidad principal de esta conducta el secuestro y la encriptación de los datos mediante el uso de sistemas informáticos para privar del acceso al titular, sino únicamente se resalta la duplicación de la información obtenida ilegalmente sin privar del acceso al usuario al que pertenece.

> *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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 231****.* Registro Oficial.)

El sujeto activo no llega a ser calificado; se considera como sujeto pasivo a la persona titular del activo patrimonial que busca ser transferido; el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; los verbos rectores son “alterar”, “manipular”, “modificar”; la pena impuesta es de tres a cinco años de ser sancionado el ilícito; el condicionante del presente delito es la alteración que se da al sistema electrónico o mensaje de datos que comete el sujeto activo sobre la víctima de este ilícito, y de acuerdo con el segundo inciso también es condicionante el proporcionar información bancaria personal para obtener activos patrimoniales de una manera contraria a la ley. Sin estos condicionantes el autor no puede proceder a realizar la transacción de los activos mencionados.

Este tipo penal abarca la utilización de sistemas electrónicos y tecnología para el cometimiento de la conducta descrita, logrando así ajustarse al presupuesto de delito informático como tal cometido por sistemas informáticos al alterar y sabotear el funcionamiento normal de los sistemas que contienen este tipo de información.

Empero, este artículo no se centra en la sanción de la encriptación de estos datos de carácter patrimonial ni en afectar el funcionamiento normal de los sistemas informáticos, sino por otra parte busca regular el fenómeno de las transferencias fraudulentas o sin consentimiento de dichos activos.

> *Art. 232.-* ***Ataque a la integridad de sistemas informáticos.-*** *(Sustituido por el Art. 13 de la Ley s/n R.O. 526-4S, 30-VIII-2021).- 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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 232****.* Registro Oficial.)

En este artículo se contempla un sujeto activo no calificado; el sujeto pasivo en este delito es la persona o grupo de personas propietarios de los sistemas informáticos afectados; el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; los verbos rectores son “destruir”, “dañar”, “borrar”, “deteriorar”, “alterar”, “suspender”, trabar”, causar mal funcionamiento”, “suprimir”, “diseñar”, “desarrollar”, “programar”, “adquirir”, “enviar”, “introducir”, “ejecutar”, “vender”, y “distribuir”; la pena impuesta es una pena privativa de la libertad de tres a cinco años;

el condicionante en el presente delito es que se vea afectada la unidad de soporte lógico del sistema informático mediante la utilización de métodos de experticia informática y no en su *hardware*, es decir en su sistema operativo o en su “software”, y no en su estructura o componentes físicos, y que además este deterioro en la integridad del equipo no sea el resultado de un deterioro físico del sistema dado previamente al cese de la totalidad de sus funciones lógicas.

En el presente artículo se toma al ataque de la integridad de los sistemas informáticos como la invasión o alteración en la integridad o contenido de la información del sistema informático como conducta sancionada por el ordenamiento. Este artículo regula parcialmente ciertos aspectos del *ransomware*, tal y como lo es el causar un funcionamiento inusual o irregular al sistema como tal o a los componentes del sistema informático, lo cual encajaría al supuesto descrito de secuestro de datos. Sin embargo, si bien el Código regula el ataque a la integridad de los sistemas, un mismo artículo no puede sancionar dos conductas distintas, puesto que la finalidad de cada uno de los tipos penales es la de sancionar o regular la conducta que describe, y el *ransomware* al poseer otros elementos que la doctrina actual sobre Delitos Informáticos contempla y que no son regulados por el Código, tal y como el resultado extorsivo que se desencadena de la implantación del virus, o la contemplación de Funcionalidad Informática como nuevo bien jurídico protegido, no se adecúa al tipo penal de ataque a la integridad de los Sistemas, y por lo tanto no puede ser sancionada mediante el presente artículo.

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. (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 233****.* Registro Oficial.)

En cuanto al primer inciso, el sujeto no es calificado; el sujeto pasivo es la sociedad en general; los verbos rectores son “destruir” e “inutilizar”, el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena que se impone es de cinco a siete años de ser sancionada la conducta; el condicionante en este tipo penal es la información que se vea afectada sea información de carácter clasificado de acuerdo a lo que el ordenamiento jurídico disponga. En el segundo inciso, el sujeto activo es calificado, llegando a ser servidores públicos; el sujeto pasivo es la sociedad en general; el verbo rector es “obtener”; el bien jurídico protegido es de igual manera la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena impuesta es de tres a cinco años; el condicionante para que sea sancionado es que el sujeto activo sea un servidor que se valga de su posición de poder para obtener dicha información. En el último inciso, el sujeto activo es calificado; el sujeto pasivo es la sociedad en general; el verbo rector es

“revelar”, el bien jurídico llega a ser, como en los incisos anteriores, la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena impuesta es una pena privativa de la libertad de siete a diez años e inhabilitación de ejercer un cargo o función por seis meses; y el condicionante es que debe determinarse que la información difundida por el servidor pueda comprometer la seguridad del Estado en general, de lo contrario no se puede aplicar la pena dispuesta.

Este artículo no resulta relevante en cuanto a la regulación del *ransomware*, debido a que su espíritu trata de regular únicamente la destrucción y sustracción de información por cualquier medio, sea físico o electrónico, cuando ésta posee protección otorgada por fuerza de la ley o por su naturaleza de ser delicada para la seguridad del Estado y de sus habitantes.

> *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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 234***. Registro Oficial.)

El sujeto activo en el primer numeral no es calificado; el sujeto pasivo es la sociedad en general; el verbo rector es “acceder”, el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena que

se determina para este caso es de tres a cinco años; el condicionante en este tipo penal es la invasión total o parcial de un sistema informático o de telecomunicaciones, sin que exista un consentimiento expreso y la voluntad de la persona, grupo de personas o entidad de permitir dicho acceso. En el segundo numeral, el sujeto activo tampoco es calificado; el sujeto pasivo es la sociedad en general; el verbo rector es “explotar”, “modificar”, “desviar”, “redireccionar”, “ofrecer”; el bien jurídico protegido es la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena con la que se sanciona este ilícito es de tres a cinco años de pena privativa de la libertad.

Dentro de este tipo penal se hace mención a los delitos que constan de obtener un acceso no autorizado en ordenadores y sistemas informáticos que desencadene en la obtención de ganancias a costa de la vulneración de Derechos de la víctima, lo cual no encuadra con el presupuesto planteado para la comisión del secuestro de datos, ya que en este tipo penal se hace exclusiva referencia al acceso no autorizado, supuesto en el que el autor del ilícito tendría que acceder manual o remotamente al contenido de la información y sacar provecho de aquello, situación que no se produce en el secuestro de datos, puesto que esta conducta priva al usuario de la lectura de la información encriptada mediante la implantación de malwares a partir de correos electrónicos u otros medios de ingeniería social, y además se produce a partir de la voluntad de la víctima obtenida por medio del engaño.

La regulación del acceso no autorizado no regula los supuestos de la implantación de virus *ransomware* para secuestro de datos que se plantean en la investigación, en el sentido que, en el acceso no autorizado a sistemas informáticos el

delincuente informático posee control total de la información y del contenido de esta, pudiendo sacar provecho de la venta o divulgación de las ideas plasmadas en sí, teniendo que intervenir directamente y con consciencia para dirigir el ataque; mientras que en el secuestro de datos el autor priva a la víctima de la disponibilidad que posee al sistema informático en todo o parte mediante la encriptación del sistema y de su información a través de la implantación de virus sin que este tenga que adentrarse en el sistema para dirigir el secuestro, poseyendo solamente el control de la liberación del ransomware que provoca el secuestro de información y que será dada a partir del pago de la cuota que se solicita como rescate.

A manera de énfasis, en el secuestro de datos el autor no dirige un ataque ni invade directamente el sistema informático con el uso de otro sistema, sino por otra parte, se hace el uso de *softwares maliciosos* previamente diseñados para cometer el ataque para el encriptado para el que fue desarrollado e instalados mediante el engaño, sin que este haya participado de forma física al momento del encriptado.

> *Art. 234.1.-* ***Falsificación informática.*** *(Agregado por el Art. 15 de la Ley s/n R.O. 526-4S, 30-VIII-2021).-*
>
> *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.* (Tomado de Asamblea Nacional, 2014. **Código Orgánico Integral Penal,** ***Título IV: Infracciones en Particular, Capítulo III, Sección Tercera, Art. 234.1****.* Registro Oficial.)

El primer numeral de este artículo establece como sujeto activo un sujeto no calificado; como sujeto pasivo se determina a la sociedad en general; como verbos rectores “provocar”, “introducir”, “modificar”, “eliminar”, “suprimir”, “interferir”; como bien jurídico protegido se coloca la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena que se impone es la privación de la libertad de tres a cinco años; el condicionante del presente delito es que el engaño o falsificación de la información sea dado para provocar un engaño o falla en relaciones jurídicas en general. En el segundo numeral el sujeto activo no es un sujeto calificado; el sujeto pasivo es la sociedad en general; el verbo rector es “causar” y “usar”; el bien jurídico protegido es de igual manera es la Seguridad de los Activos de los Sistemas de Información y Comunicación; la pena es la misma que se impone en el numeral anterior; el condicionante es la utilización de los documentos que se generan en el supuesto fáctico del primer numeral.

Este tipo penal no llega a ajustarse a ser un Delito Informático al no afectar la funcionalidad informática de sistemas informáticos de los cuales de obtiene la documentación falsificada, ni tampoco es su fin el tipificar el robo de esta información. El mismo artículo en su segundo inciso indica una sanción similar para la utilización de los documentos generados en la falsificación, lo cual no afectaría en ninguna manera el funcionamiento de ningún ordenador.

3. Capítulo III: El análisis del *Ransomware* o Secuestro de Datos como delito en el ordenamiento jurídico ecuatoriano

En este punto es necesario hacer una recapitulación de las ideas desarrolladas en los apartados anteriores para obtener un panorama más claro de lo que se quiere conseguir de esta investigación. Para comenzar, se debe señalar que a través del análisis y desarrollo del primer capítulo se pudo obtener una conceptualización y definición de lo que se define por Secuestro de Datos o *Ransomware*, su clasificación mayormente aceptada por la doctrina, su modalidad y las implicaciones y consecuencias que desencadenan para los involucrados. En el Segundo se realizó un análisis del tipo penal de los delitos informáticos que son regulados en el catálogo de delitos del Código Orgánico Integral Penal dentro del cual se destacaron los elementos del tipo penal como sujeto activo, sujeto pasivo, bien jurídico protegido, verbo rector, pena, y el condicionante del delito.

Ahora, es importante destacar que el objetivo de esta investigación es el determinar si el Código Orgánico Integral Penal abarca en su tipificación el *Ransomware* o Secuestro de Datos, puesto que ha sido una conducta que ha venido en auge tras la automatización y la sistematización de la sociedad hasta el punto de convivir cotidianamente con sistemas informáticos y con inteligencias artificiales.

A manera de comentario personal, resulta conveniente señalar un par de aspectos y características del Derecho. Este está basado en una Función Social, es decir en ayudar a la sociedad mediante la regulación, tipificación o sanción de determinados hechos o situaciones, y su contenido será promulgado y aprobado para obtener una armonía social, y no para el beneficio de ciertos grupos de poder. Por otra

parte, otra característica del Derecho es el ser un mecanismo dinámico, es decir, que está en cambio y transformación constante conjuntamente con la sociedad sobre la cual debe desprender leyes y normas, por lo que los legisladores deben buscar una actualización constante de la legislación en base a los fenómenos sociales producidos en el territorio para controlarlos y que la Ley imponga su poder sobre dichas situaciones, de modo que el desarrollo del Derecho y la sociedad sea posible.

Dadas estas dos premisas, considero que el Derecho Penal en nuestro país debe ir a la par de todos los fenómenos que se producen diariamente en nuestra sociedad, incluyendo el surgimiento de nuevas conductas delictivas que son cometidas mediante el uso de sistemas informáticos, y en general que se considere como un delito informático, ya que de no hacer frente a esta problemática las consecuencias pueden comprometer los derechos de los ciudadanos y a la seguridad del mismo Estado dado que estos delitos necesitan únicamente una conexión a internet para que sean efectuados.

3.1. Algunas consideraciones constitucionales y normativas sobre los Delitos Informáticos en el Ordenamiento Jurídico ecuatoriano

Además del Código Orgánico Integral Penal y su regulación, el ordenamiento jurídico ecuatoriano contiene otros cuerpos normativos que se encargan de regular de cierta forma la información, el uso de la tecnología, el comercio electrónico, y demás aspectos que se reglamentan tanto en la Constitución de la República en su catálogo de Derechos Fundamentales como en la Ley de Comercio Electrónico, Mensajes de Datos y Firmas electrónicas aprobada en el año de 2002, notando así que dentro del Estado ya ha dado por iniciada una campaña que busca la regulación y la minimización

de Delitos Informáticos en el territorio desde hace ya casi dos décadas. (Ortiz Campos, 2019)

Es importante que a este tipo de problemáticas relacionadas con la aparición de la tecnología y las inteligencias artificiales se le dé un tratamiento en todo el ordenamiento jurídico, empezando por otorgar un catálogo de derechos humanos que tiendan a proteger el acceso a las mismas, además de cubrir aspectos como de brindar conceptos básicos, reglas básicas y una serie de regulaciones específicamente creadas para este efecto, con el apoyo de otras áreas como de la informática para el desarrollo de material doctrinario y legal, la sociología para poder establecer fenómenos sociales y patrones de conducta tanto en la población afectada para establecer falencias en la seguridad de sus ordenadores.

> En la Constitución de la República del Ecuador del 2008 en su artículo 16 se manda lo siguiente:
>
> "Art. 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
>
> (…) 2. El acceso universal a las tecnologías de información y comunicación." (Tomado de Asamblea Nacional Constituyente, 2008. ***Constitución de la República del Ecuador, Título II: Derechos, Capítulo II, Sección Tercera, Art. 16.*** Registro Oficial)

Dentro de este artículo nuestros legisladores han colocado al acceso universal a las tecnologías de la información y la comunicación como un Derecho Fundamental. Cabe recalcar que los Derechos consagrados en la Constitución están revestidos de una protección otorgada por la jerarquía normativa dentro del Estados ecuatoriano, ya

que estos están sobre cualquier otra normativa o ley, incluyendo que los cuerpos normativos creados posteriormente y que regulen este ámbito.

En esa misma línea Atencio-González et al. (2022) realiza un ensayo sobre los Derechos Fundamentales de carácter Colectivo, en el cual señala que los derechos sean individuales o colectivos merecen la misma protección y tutela por parte del Estado y sus dependencias. Empero, un derecho individual al resultar afectado únicamente desemboca en un deterioro a la situación de una única persona, siendo más fácil y personalizado el tratamiento que se le da cuando este se ve vulnerado, a diferencia de los derechos fundamentales colectivos, que al momento en el que son comprometidos pueden llegar a causar afecciones a un grupo o grupos de personas determinado, en ciertos casos siendo grupos de atención prioritaria, llega a significar un trabajo más complejo el reparar los daños cometidos por el menoscabo de estos derechos, debido a que al afectar a la colectividad se deben emplear más recursos para poder resarcir los daños de todos los involucrados. De esta manera al ser el artículo 16 un derecho de la colectividad merece que el Estado se comprometa a realizar cualquier acción dirigida a su protección directa e inmediata, por lo que cualquier acto que desemboque en la privación de este derecho hacia una persona o grupo de personas será sancionado de la manera más oportuna y conforme a la Ley.

Así mismo, la Constitución de la República contempla lo siguiente:

> Art. 17.- EI Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:
>
> (…) 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como **el acceso universal a las tecnologías de información y comunicación** en especial para las personas y

colectividades que carezcan de dicho acceso o lo tengan de forma limitada. (Tomado de Asamblea Nacional Constituyente, 2008. ***Constitución de la República del Ecuador, Título II: Derechos, Capítulo II, Sección Tercera, Art. 17.*** Registro Oficial)

En el presente artículo citado se hace alusión al papel que posee el Estado para garantizar el acceso universal a las tecnologías ya mencionadas. En estos apartados se utiliza el término facilitar, por medio del cual entendemos que el Estado velará por el libre acceso de todos los ciudadanos del territorio este Derecho y tomará las acciones correspondientes para que esto sea posible. Para poder proteger estos derechos es menester que además de otorgar un carácter de Derecho Fundamental al acceso a las tecnologías, también se elabore una legislación que se encargue de regular en su totalidad a los nuevos delitos informáticos suscitados que afectan netamente a la funcionalidad informática de los sistemas, y no únicamente regulando saboteos físicos a los ordenadores, o delitos cometidos empleados con computadores como herramientas no prescindibles para llegar a su cometido.

Por otra parte, la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas es una normativa creada en el año 2002, en la cual contiene definiciones de mensajes de datos, comercio electrónico, firmas electrónicas, además de desprender elementos de los mismos y un catálogo de conductas que con posterioridad llegarían a ser parte del actual y vigente Código Orgánico Integral Penal. Además de ofrecer estas disposiciones, esta ley se basaba principalmente en la protección de los usuarios de estos medios electrónicos, puesto que al ser de este tipo carecen de una tutela física por parte del Estado y las autoridades, y de esta forma se promovió una iniciativa en la que se tomó con mayor seriedad a las actividades que involucraban el

uso de sistemas electrónicos o del tránsito electrónico de mensajes de datos. (Ortiz Campos, 2019)

De esta manera, al analizar estos cuerpos normativos podemos destacar una preocupación por parte del Estado en relación a la regulación de los delitos cometidos por medios informáticos, incluso hasta antes de la aprobación de la Constitución del 2008, ofreciendo disposiciones de carácter constitucional que protegen el acceso libre y voluntario de los ciudadanos a las nuevas tecnologías, sin que ningún agente prive o sabotee su experiencia para provocar un menoscabo en su integridad y facilitando todos los medios para que esta sea una realidad y no únicamente se encuentre plasmado en papel; también otorgando una conceptualización de los mensajes de datos y del alcance de la protección de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas a los usuarios de este tipo de tecnologías.

3.2. El acceso a las tecnologías de la Información y Comunicación como Derecho Humano en la actualidad

En mi consideración, la aparición de las nuevas tecnologías ha desembocado en que varias personas se vean en el papel de aprender a emplearlas dentro de su vida diaria, en aspectos tan básicos como pagos de servicios básicos, almacenamiento de información, por lo que los Estados al notar esta particularidad en la sociedad por medio de Convenciones y Tratados han logrado incluir al acceso libre y universal a estas tecnologías como un Derecho Humano, dando así disposiciones y recomendaciones no obligatorias sobre cómo regular esta situación en sus ordenamientos con directrices y guías establecidas bajo la presentación de contextos sociales de los Estados parte, logrando así ofrecer una protección a las personas que

prescinden de estos artefactos, incluyendo al Estado mismo en sus diversas áreas de trabajo cuando hace uso de sistemas informáticos y tecnologías de la información y comunicación para lograr ejecutarlas.

El jurista Moranchel Pocaterra (2019) desarrolla la idea de que el derecho al acceso a estas tecnologías además de ser un derecho humano resulta un derecho habilitante para otros de la misma jerarquía; un derecho habilitante es aquel que resulta indispensable para que otros derechos puedan hacerse efectivos en su totalidad, tal y como lo asevera con ciertos derechos como el de la libertad de expresión, o como la educación, siendo así que, debido al contexto social que se vive actualmente, para que una persona pueda hacer uso de su libertad de expresión el Estado deberá facilitar y garantizar los medios adecuados para que este pueda desenvolverse libremente por medio de ellos, siendo limitado únicamente por los derechos y las libertades del resto de personas que habitan en el mismo territorio; asimismo una educación de calidad en la actualidad puede ser ofrecida mediante el uso de la tecnología como herramienta para complementar y auxiliar los procesos de aprendizaje y de desarrollo cognitivo de las personas en sus diversas etapas, desde la educación básica hasta la formación profesional del individuo. (pp. 512-514)

Al ser un derecho habilitante para que otros puedan cumplirse con efectividad, la inclusión del derecho humano al acceso a las tecnologías de la información y la comunicación es una clara muestra que la sociedad ecuatoriana actual enfrenta un cambio cultural al palpar la incorporación de la tecnología y los sistemas informáticos dentro de los procesos más básicos hasta los más complejos del ser humano, y a su vez el ordenamiento jurídico y los legisladores se enfrentan a este cambio teniendo

cada vez más que estudiar e instruirse sobre los nuevos peligros que acarrea para la colectividad las actividades tanto legales como delictivas que puede involucrar el uso de estas tecnologías.

Otro reto por el que se vieron involucrados la totalidad de los Estados del mundo fue el de la pandemia por el virus COVID-19, situación que desembocó en el confinamiento total de las personas, afectando a las actividades laborales, educativas, personales y demás de las personas, generando así una situación en la que la tecnología fue el único medio para llevar con normalidad estas actividades y que no haya un colapso en las familias y en la sociedad en general. Debido a este fenómeno la educación se vio puesta en experimentos con la tecnología, mediante los cuales tantos los docentes como los Ministerios o Departamentos encargados de esta área en los Estados tengan que facilitar el acceso a estas tecnologías a todas las personas y garantizar una protección para que no se dé una privación arbitraria a este derecho, teniendo así los docentes que innovar las técnicas de enseñanza y ajustarse a la virtualidad y el Estado de garantizar el derecho a la educación por estos medios. Tras este fenómeno, la virtualidad vino de la mano con la creación de una serie de modalidades de trabajo, técnicas de educación y demás actividades basadas en esta modalidad, haciendo que, aunque las restricciones por la pandemia sean retiradas, no se ponga en riesgo la estabilidad de los usuarios de servicios virtuales y algunas actividades puedan ser continuadas mediante la virtualidad. (Cotino Hueso, 2020)

Así podemos evidenciar que las tecnologías de la información y comunicación y los ordenadores han llegado a formar parte del Derecho y de las regulaciones que cada Estado elabora de acorde a su realidad, por lo que es menester que estas regulaciones

se encuentren en constante estudio y tratamiento por la facilidad con la que nuevas variantes y modalidades de delitos informáticos pueden llegar a aparecer, significando un reto cada vez más complejo para nuestros legisladores. Por ende, es obligación de los mismos en la utilización de recursos y medios de estudio e investigación siempre está presente, ya que de no hacerlo a cabalidad se estaría poniendo en juego la seguridad jurídica de las personas y de igual manera a los derechos consagrados en la Constitución.

3.3. Contrastación de la información analizada en la investigación

Del análisis del tipo penal realizado a los artículos del Código Orgánico Integral Penal que se pueden identificar como delitos informáticos, se ha logrado identificar a cuatro de ellos como los que mayormente se asemejan a la modalidad de comisión del *Ransomware* o Secuestro de Datos y que se acercan a una regulación ya prevista por los legisladores para el caso. Se hará una comparación entre los delitos informáticos y la modalidad de comisión del *Ransomware* o Secuestro de Datos para determinar diferencias y similitudes que respondan a la interrogante planteada en la investigación si dicha conducta se encuentra o no bajo el alcance del ordenamiento jurídico ecuatoriano A continuación, enumeraremos y analizaremos a detalle los delitos informáticos mencionados*:*

3.3.1. Artículo 230 del Código Orgánico Integral Penal: Interceptación Ilegal de Datos

Dentro del presente artículo se pudo examinar cuatro tipos de conductas relevantes para el tratamiento de los delitos informáticos: la primera es la desviación, grabación, o filtración de cualquier tipo de información a la que la ley le ha otorgado un

carácter protegido ante el conocimiento público, la segunda es aquella conducta en la que se crean mensajes o correos falso que intentan hacerse pasar por entidades verificadas, los cuales redireccionan a los usuarios a páginas no confiables en la que se solicitan datos de carácter bancario, entre otros; la tercera es la clonación o interceptación de datos contenidos en cualquier dispositivo que involucre la integridad de tarjetas de crédito y los derechos o activos de sus titulares; por último se sanciona a aquellos que se encarguen del desarrollo y distribución de *softwares* o dispositivos creados con el fin de obtener la consecución de cualquiera de las conductas mencionadas anteriormente. Dentro de todas ellas el bien jurídico protegido es la Seguridad de los activos de los Sistemas de Información y Comunicación.

Ahora, cabe señalar la segunda y tercera conducta regulada por el presente artículo: el engaño que producen los ciberdelincuentes a sus víctimas para que ingresen datos personales y financieros en portales web no confiables; y la utilización de sistemas de clonado de las tarjetas de crédito. En estos dos apartados se hace presente el uso de sistemas informáticos u ordenadores, lo cual cumple con el presupuesto señalado al inicio de esta investigación que aseveraba que Delito Informático es el término por el que se define a aquellos que son cometidos con el uso de sistemas informáticos contra otros sistemas informáticos. Sin embargo, la segunda conducta se asemeja a lo que se pudo analizar en su momento como "*phishing"*, que es básicamente el envío de mensajes engañosos con el fin que el usuario sea redireccionado hacia portales web o sitios que contienen campos que requieren información delicada para su titular.

Con este fundamento, este artículo si bien se acerca a lo que conceptualizamos por delito informático, e incluso si bien regula la conducta *phishing*, el objeto de esta investigación es determinar si regula o no el *ransomware*, y el presente artículo no cumple con este requisito ya que norma otra conducta totalmente distinta en cuanto a su método de comisión, siendo el *ransomware* un malware que sirve para secuestrar datos que tiene como bien jurídico protegido según la jurista Mayer Lux (2018) la Funcionalidad Informática de los sistemas informáticos afectado, y el *phishing* la recolección de información mediante mensajes engañosos que vulneran netamente la Seguridad de los Activos de los Sistemas de Información y comunicación.

3.3.2. Artículo 231 del Código Orgánico Integral Penal: Transferencia Electrónica de Activo Patrimonial

En el presente artículo se describen dos clases de conductas, la cual únicamente la del primer inciso está relacionada propiamente con el uso de sistemas informáticos y con la categoría de Delito Informático. Esta actividad tipificada hace referencia a la situación en la que el ciberdelincuente por cualquier clase de medio se inmiscuye en el funcionamiento regular de sistemas informáticos, telemáticos o de datos para asegurar la transferencia de datos o directamente de dinero o activos de la víctima, siendo una especie de invasión a los sistemas para procurar dicha transferencia inmediata, sin esperar la participación de la víctima para aquello. El bien jurídico afectado en esta situación es la Seguridad de los Activos de los Sistemas que resulten afectados.

Si bien este artículo regula la transferencia no consentida de dichos activos, se tiene como bien jurídico principal la Seguridad de estos sistemas, y mas no su

Funcionalidad como tal. Es importante volver a señalar que en los delitos informáticos propios se ve afectada la Funcionalidad de los Sistemas, y en el presente la regulación desarrollada solamente señala a la seguridad y la brecha que se genera para la transferencia de datos o activos.

El *ransomware*, a diferencia de este artículo, comprende la situación en la que la víctima a base de engaños accede inconscientemente a crear una brecha en la que el ciberdelincuente puede instalar su ordenador este *malware* para el encriptado total o parcial del sistema, afectando el cómo el sistema desempeña ordinariamente sus funciones lógicas, sin involucrar la extracción de dicha información para obtener lucro a costa de ella. En pocas palabras, el *ransomware* al encriptar el sistema no extrae la información contenida, tal y como lo es el caso del presente artículo.

Con este argumento me sirvo en determinar que la regulación que el presente Código emite en su artículo 231 para la Transferencia Electrónica de Activo Patrimonial es insuficiente para cubrir con la conducta de Secuestro de datos por medio de malware *ransomware*, debido a que el Código sanciona únicamente al acto de sustracción de información sin importar que este inutilice o afecte el funcionamiento de los Sistemas Informáticos invadidos, y el *ransomware* como conducta delictiva comprende otros enfoques como el engaño al usuario por medio de ingeniería social, la instalación de programas de código malicioso, la afectación de la Funcionalidad Informática como bien jurídico protegido, y la extorsión que se provoca a la víctima para el desencriptado de la información.

3.3.3. Artículo 232 del Código Orgánico Integral Penal: Ataque a la Integridad de Sistemas Informáticos

Este artículo resulta ser el Delito Informático por excelencia tipificado dentro de nuestro Código Orgánico Integral Penal vigente, puesto que involucra directamente las afecciones a la integridad y en el funcionamiento del soporte lógico de los sistemas informáticos o de tratamiento de información, dejando de lado aspectos patrimoniales y físicos relacionados con el *hardware* o los componentes físicos de dichos sistemas. En su contenido se sirve en tipificar cualquier acto que esté destinado al deterior total o parcial en la integridad de los ordenadores o sistemas, además de incluir la sanción a la creación de métodos, programas o demás técnicas encaminadas a lograr lo mencionado anteriormente, por lo que se podría decir que hay una regulación parcial de esta conducta.

A simples rasgos podríamos deducir que la presente regulación se extiende hasta el punto de sancionar el secuestro de datos, lo cual resulta erróneo puesto que la doctrina misma ha desarrollado material y elementos que asevera que las legislaciones deben recabar para regular esta conducta de una manera eficaz, por lo que, al no hacerse mención a la modalidad extorsiva del *ransomware*, ni a la Funcionalidad Informática como bien jurídico protegido en lugar de la Seguridad de los Activos de dichos Sistemas, y al no poder regular un tipo penal dos conductas distintas, me sirvo a manera de conclusión del análisis de este artículo aseverar que el presente tipo penal no regula la conducta de Secuestro de Datos.

3.3.4. Artículo 234 del Código Orgánico Integral Penal: Acceso no consentido a un Sistema Informático, Telemático o de Telecomunicaciones

Este artículo se centra en el acceso no consentido que una persona realice dentro de un ordenador o sistema informático de una tercera persona, con el fin de obtener un beneficio para sí mismo bajo el uso ilegítima de los mensajes, información contenida en los sistemas, o con el mero uso del sistema como tal para obtener gananciales. Se tratan dos tipos de conductas: el acceso no consentido al sistema informático; y además la utilización de dicho acceso para obtener provecho en perjuicio de los derechos del legítimo dueño del sistema. El Código Orgánico Integral Penal aprobado por la Asamblea Nacional de la República del Ecuador (2014) en dicho artículo menciona a la "explotación ilegítima" de aquellos mensajes obtenidos e información proveniente de la memoria de los sistemas informáticos invadidos. Resulta ambiguo el interpretar lo que se determina como "explotación ilegítima", sin embargo, aseveraremos según su etimología que, es el obtener un acceso no autorizado dentro de un sistema informático que desemboque en la obtención de beneficios económicos a costa de los derechos de la víctima, lo cual es totalmente incompatible con la conducta del secuestro de datos.

Para argumentar dicha posición analizaremos los siguientes aspectos: a) el tipo penal hace referencia al Acceso No Autorizado a sistemas y en el *ransomware* el autor no accede al sistema afectado de ninguna forma, sino que mediante la instalación del *malware* dentro del sistema *se* realiza el secuestro; y b) en el articulado se coloca como bien jurídico protegido la Seguridad de los Activos de los Sistemas de Información y Comunicación, mientras que la doctrina asevera que la funcionalidad del sistema

informático es aquello que debería ser tomado en cuenta como bien jurídico en delitos informáticos y en el ransomware en especial, conducta que afecta directamente la funcionalidad del sistema informático mediante la privación de la lectura y acceso al mismo sin afectar la integridad de la información del mismo ni accediendo a ella.

3.4. Verificación de la Hipótesis

¿Cómo el Código Orgánico Integral Penal regula la conducta del Ransomware (Secuestro de Datos) en su catálogo de delitos?

Para poder responder a la hipótesis planteada al principio de esta investigación se realizó un análisis doctrinario del *ransomware* como conducta penalmente relevante para la doctrina, investigando sus características y elementos, conjuntamente con el desarrollo de un análisis del tipo penal de aquellos delitos que se ajustan al presupuesto de Delitos Informáticos cometidos a través de sistemas informáticos hacia otros sistemas de la misma índole.

Al dar por terminado este análisis podemos determinar que, si bien nuestro Código ofrece una serie de regulaciones destinadas a la sanción y prevención de delitos informáticos, estos no se encuentran lo suficientemente desarrollados para poder categorizar al secuestro de datos como conducta ilícita en su contenido, ya que se dejan de lado aspectos como la funcionalidad de los sistemas informáticos como centro de la problemática, tal y como han desarrollado juristas en sus obras y se da mayor importancia al deterioro de los componentes físicos y de los datos almacenados al momento de la creación de un catálogo de delitos informáticos.

Es menester tener presente que en nuestro ordenamiento jurídico se aplica una regla de interpretación restrictiva en la normativa penal, por lo que únicamente se sancionará al autor de una conducta si esta se encuentra tipificada con todos sus elementos, y no se castigará a una misma conducta con dos tipos penales diferentes, ya que cada tipo está creado para sancionar una sola conducta con sus variantes.

Con este fundamento y respondiendo a la hipótesis planteada al inicio de la investigación, el Código Orgánico Integral Penal recae en una falta de tipificación de la conducta de *Ransomware* (Secuestro de Datos), al no tomar en cuenta aspectos de la diferenciación de la modalidad de comisión del delito y de la doctrina desarrollada en los últimos años para el tratamiento de los delitos informáticos y de este supuesto en específico.

CONCLUSIONES

Tras haber dado por concluida la presente investigación, de los capítulos desarrollados podemos obtener los siguientes resultados:

a) Del primer capítulo, pudimos deducir que el *Ransomware* es el término acuñado para definir a la conducta de Secuestro de Datos, y que de igual manera es empleado para reconocer al *software malicioso* programado para el encriptado parcial o total de la información contenida en el sistema informático afectado para solicitar un monto o retribución económica para la liberación de su ordenador; además que existen varias clases de *ransomware* desarrolladas para cumplir con secuestros de datos cumpliendo con distintas modalidades; de igual manera se analizó a la “Funcionalidad Informática” como nuevo bien jurídico protegido desarrollado por la doctrina dentro de los Delitos Informáticos, estableciendo los daños al soporte lógico del sistema operativo como un nuevo punto de interés para el Derecho, ajeno de a los daños materiales o al *hardware* del equipo ya considerados por la legislación y la doctrina; de igual manera se pudo examinar Tratados Internacionales y Legislación Comparada con la legislación Peruana y la legislación Española, con lo que pudimos determinar que en otros ordenamientos se ha dado un tratamiento a esta problemática.
b) En el segundo capítulo pudimos identificar que en nuestro ordenamiento jurídico sí existe una preocupación por parte de los legisladores en normar estas nuevas conductas informáticas ilícitas, puesto que el Código Orgánico Integral Penal acoge cierta regulación destinada a sancionar delitos en los cuales se ve involucrado directamente el uso de sistemas electrónicos o informáticos como

herramientas importantes para el desempeño estos dichos actos, tal y como lo es el caso de los delitos en contra de la Seguridad de los Activos de los Sistemas de Información y Comunicación, y de los artículos 232 y 234 en específico del mismo cuerpo normativo, puesto que emplean ciertos parámetros de la corriente dada por la doctrina de colocar a la funcionalidad de los sistemas como parte del debate de los elementos de los delitos informáticos, estableciendo diferencias entre las afectaciones a la integridad de los datos del sistemas de las vulneraciones a la funcionalidad del sistema, como lo es la función de lectura y disponibilidad de la visualización en el monitor de los procesos lógicos realizados en los ordenadores.

c) Como conclusión del tercer capítulo, tras realizar una comparación entre los resultados obtenidos en la investigación de los capítulos anteriores, se pudo determinar que nuestro ordenamiento no regula el *ransomware* debido a que la legislación nacional no contempla aspectos doctrinales necesarios para dicho efecto; que en nuestro ordenamiento jurídico se da relevancia constitucional al Derecho al acceso a las nuevas tecnologías; y que el Estado por tal motivo debe garantizar los medios para hacer efectivo este derecho habilitante, por lo que debe otorgar de manera inmediata una regulación para sancionar y prevenir aquellas conductas que desencadenan en una privación al libre ejercicio de este Derecho de Acceso Universal a las Tecnologías de Información y Comunicación, el cual se encuentra reconocido en Tratados Internacionales ratificados por el Estado ecuatoriano.

RECOMENDACIONES

Como principal recomendación hago un llamado a los legisladores a que contemplen la posibilidad de la creación de un tipo penal propiamente diseñado con el fin de abarcar todos los aspectos doctrinales y prácticos que el secuestro de datos implica, principalmente debido a la interpretación restrictiva propia de la materia, y colocar a la Funcionalidad Informática propuesta por otros juristas como un bien jurídico protegido por el ordenamiento jurídico.

También considero que es importante el desarrollar continuamente material doctrinario que pueda complementar la tarea de la tipificación de estas nuevas conductas de delincuencia informática, tal y como lo es en el caso del desarrollo de la "Funcionalidad Informática" como parte de la nueva doctrina para determinar nuevos bienes jurídicos protegidos en los Delitos Informáticos, lo cual ha servido como pauta para que muchos Estados opten por tomar en cuenta la afectación a la integridad de dichos sistemas o su correcto funcionamiento como una nueva vulneración de derechos, aparte de los detrimentos físicos de los equipos o de los activos patrimoniales contenidos en ellos.

Además, es tarea del mismo Estado el realizar campañas o charlas de concientización sobre delincuencia informática, logrando así una intervención en la sociedad para explicar los peligros e implicaciones que se desenvuelven de los delitos cometidos por medios informáticos, ya que la sociedad en general se encuentra en vulnerabilidad ante esta situación al tener libre acceso a la tecnología y a la conectividad por redes.

BIBLIOGRAFÍA

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, *25*(89). https://doi.org/10.37960/revista.v25i89.31534

Asamblea Nacional Constituyente de la República del Ecuador. (2008). Constitución del Ecuador. In *Registro Oficial* (Vol. 449). http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf

Asamblea Nacional de la República del Ecuador. (2014). Código Orgánico Integral Penal. In *Registro Oficial - Órgano del Gobierno del Ecuador*.

Atencio-González, R. E., Castro-Núñez, W. E., Castro-Zambrano, J. W., & Torres-Parreño, A. N. (2022). Derechos humanos colectivos en los ciudadanos ecuatorianos. *Cienciamatria*, *8*(1), 200–205. https://doi.org/10.35381/cm.v8i1.663

Bacigalupo Saggese, S., Bajo Fernández, M., Basso, G. J., Cancio Meliá, M., Díaz-Maroto y Villarejo, J., Fakhouri Gómez, Y., Lascuraín Sánchez, J. A., Maraver Gómez, M., Mendoza Buergo, B., Molina Fernández, F., Peñaranda Ramos, E., Pérez Manzano, M., Pozuelo Pérez, L., & Rodríguez Horcajo, D. (2019). Manual de Introdución al Derecho Penal. In *Agencia Estatal Boletín del Estado*. https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DP-2019-110

Barker, W. C., Barker, W. C., & Fisher, W. (2022). Gestión de riesgo de ransomware : Gestión de riesgo de ransomware : *National Institute Of Standards and Technology. U.S. Department of Commerce*, *NISTIR 837*.

Centro Criptológico Nacional. (2016). Medidas de seguridad contra ransomware. Ley

CCN-CERT IA-11/18. In *Ministerio de la Presidencia y para las Administraciones Futuras*. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1384-ccn-cert-ia-01-16-medidas-de-seguridad-contra-ransomware/file.html

Congreso de la República. (2013). *Ley N° 30096 - Ley de Delitos Informáticos*. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Consejo de Europa. (2004). *Convenio de Budapest sobre la Ciberdelincuencia*.

Cornejo Arismendi, J. (2021). Criminalidad Informática y la Discusión sobre el Bien Jurídico Protegido en los Delitos Informáticos. *Repositorio Pontificia Universidad Católica Del Perú*. https://repositorio.pucp.edu.pe/index/handle/123456789/182684

Cotino Hueso, L. (2020). La enseñanza digital en serio y el derecho a la Educación. *Revista de Educación y Derecho*, *21*, 1–29. https://dialnet.unirioja.es/servlet/articulo?codigo=7388655

Echeverría, H., Abad, A., & Ramos, V. (2019). Algunas Consideraciones Sobre La Tipicidad En La Teoría Del Delito. *Universidad y Sociedad*, *9*(2), 313–318. http://scielo.sld.cu/pdf/rus/v12n4/2218-3620-rus-12-04-265.pdf

Espinoza Coila, M. (2018). El Derecho Penal Informático Humano Como Cautela Frente Al Poder Punitivo En La Sociedad De Control. *Revista De Derecho*, *3*(2), 233–245. https://doi.org/10.47712/rd.2018.v3i2.26

Estrada Cola, C. (2018). *Estudio sobre el malware Ransomware*. Universitat Oberta de Catalunya (UOC).

Fuentes Marrufo, T., Mazún Cruz, R., & Cancino Méndez, G. (2017). Perspectiva sobre los delitos informáticos : un punto de vista de estudiantes del Tecnológico Superior Progreso. *Advances in Engineering and Innovation*, *2*(4), 1–8. http://www.progreso.tecnm.mx/revistaAEI/index.php/aei/article/view/20

Gonzales, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). Delitos Informáticos: Una Revisión en Latinoamérica. *Conference Proceedings*, *2*(1), 178–190.

Macías-lara, R. A., Fabricio, M., Andrade, B., Angulo, F. Q., Javier, J., Loor, M., & Estupiñan-troya, G. (2022). *Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática*. *3*, 231–243.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. In *Revista Chilena de Derecho* (Vol. 44, Issue 1).

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159–206. https://doi.org/10.4067/s0718-00122018000100159

Moranchel Pocaterra, M. (2019). El derecho humano al acceso y uso de las TIC como derecho habilitante. *Revista de La Facultad de Derecho de México*, *69*(274–1), 505. https://doi.org/10.22201/fder.24488933e.2019.274-1.69966

Moreno, J., Rodriguez, C., & Leguias, I. (2020). Revisión sobre propagación de ransomware en sistemas operativos Windows. *I+D Tecnológico*, *16*(1), 39–45. https://doi.org/10.33412/idt.v16.1.2438

Ortiz Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador.

Revista Científica Hallazgos21, *4*(April).

Romano Ozcáriz, D. (2019). Análisis Criminológico de los Ataques DDoS - Una Propuesta de Lege Ferenda. In *Universidad de Alcalá*.

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis Conceptual del Delito Informático en Ecuador. *Revista Conrado*, *17*(78), 343–351.

Solano Vélez, H., Duque Pedroza, A., & Díez Rugeles, M. (2019). Temas de derecho penal parte general. Teoría general del derecho penal. In *Editorial Universidad Pontificia Bolivariana*.

Téllez Valdés, J. (2009). *Derecho Informático: Cuarta Edición*. Instituto de Investigaciones Jurídicas Universidad Nacional Autónoma de México. https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf

Trigo, S., Castellote, M., Podestá, A., Ruiz De Angeli, G., Lamperti, S., & Constanzo, B. (2017). *Ransomware: seguridad, investigación y tareas forenses*. http://www.info-lab.org.ar

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2019). Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *E17*, 671–677. https://search.proquest.com/openview/b7f8919dbb75fa3e5f21552a48e94816/1?pq-origsite=gscholar&cbl=1006393%0Ahttps://search.proquest.com/docview/2195127299?pq-origsite=gscholar&fromopenview=true

Zambrano Pasquel, A. (2021). Teoría del Delito y Tentativa. *Revista de La Facultad de Derecho y Ciencias Sociales de La Universidad Nacional Del Nordeste*, *3 Num. 5*, 23. http://jorgemachicado.blogspot.com/2009/02/que-es-el-delito.html

ANEXOS:

Universidad Católica de Cuenca	AUTORIZACIÓN DE PUBLICACIÓN EN EL RESPOSITORIO INSTITUCIONAL	CÓDIGO: F – DB – 34 VERSION: 01 FECHA: 2021-04-15 Página 1 de 1

Fredi Gustavo Jara Cabrera, portador de la cédula de ciudadanía N.° **0105120265**. En calidad de autor y titular de los derechos patrimoniales del trabajo de titulación: **"Análisis de la falta de tipificación de la conducta: Ransomware (Secuestro de Datos) en el Código Orgánico Integral Penal**, de conformidad a lo establecido en el artículo 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, instransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de este trabajo de titulación en el Repositorio Institucional de conformidad a los dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior

Cuenca, 06 de septiembre de 2022.

F: .....

Fredi Gustavo Jara Cabrera

C.I. **0105120265**