UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

Tratamiento jurídico de los delitos informáticos en el Ecuador

AUTORA:

Espinoza Jurado Sindy Fernanda

Trabajo de titulación previo a la obtención del título de ABOGADA DE LOS TRIBUNALES Y JUZGADOS DE LA REPÚBLICA DEL ECUADOR

TUTOR:

Ab. Ycaza Mantilla Andrés Patricio, Mgs

Guayaquil, Ecuador

04 de marzo del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Espinoza Jurado Sindy Fernanda** como requerimiento para la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador.**

TUTOR

f. _____

Ab. Ycaza Mantilla Andrés Patricio, Mgs

DIRECTOR DE LA CARRERA

f. _____

Ab. Lynch Fernández María Isabel

Guayaquil, 4 de marzo del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Espinoza Jurado Sindy Fernanda**

DECLARO QUE:

El Trabajo de Titulación, **Tratamiento jurídico de los delitos informáticos en el Ecuador,** previo a la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, 4 de marzo del 2019

LA AUTORA

f. _____

Espinoza Jurado Sindy Fernanda

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Espinoza Jurado Sindy Fernanda**

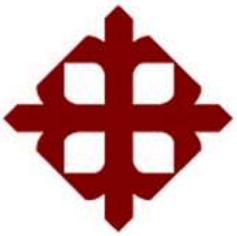
Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Tratamiento jurídico de los delitos informáticos en el Ecuador,** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, 4 de marzo del 2019

LA AUTORA:

f. _____

Espinoza Jurado Sindy Fernanda



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

Dr. José Miguel García Baquerizo, Mgs.

DECANO

f. _____

Ab. Paola Toscanini Sequeira, Mgs.

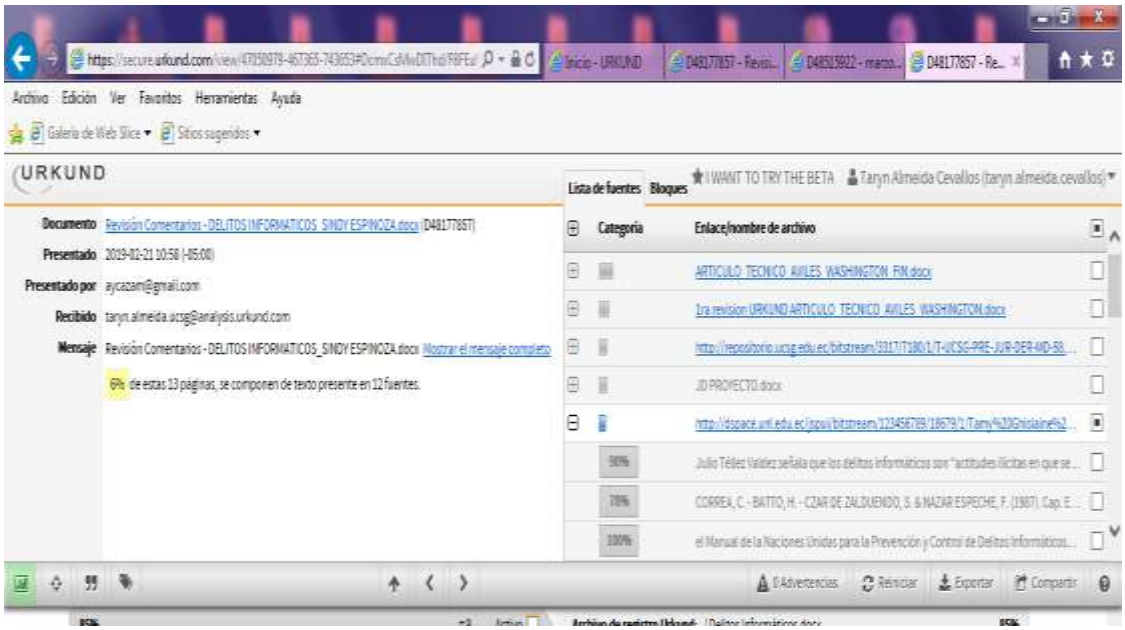
COORDINADORA DEL ÁREA

f. _____

Ab. María Patricia Íñiguez Cevallos, Mgs.

OPONENTE

REPORTE DE URKUND



TUTOR (A)

_____

Ab. Ycaza Mantilla Andrés Patricio, Mgs

AUTORA:

_____

Andrea Estefanía Villagómez Armijo.

ÍNDICE

RESUMEN (ABSTRACT)

El presente ensayo tiene como propósito el análisis sobre el tratamiento jurídico de los nuevos delitos que han surgido en los últimos años conjuntamente con la evolución de la tecnología denominados delitos informáticos; los cuales pueden ser cometidos en tiempo real, utilizando únicamente un equipo informático y sin estar presente físicamente en el lugar de los hechos.

En nuestro país el Código Orgánico Penal Integral – COIP, establece los delitos en el área informática de forma independiente y autónoma, en diferentes secciones. La tipificación este tipo de delitos en el Código Orgánico Integral Penal Ecuatoriano ha permitido sancionar los actos ilícitos con penas privativas de libertad para diferentes actores de la seguridad informática, que van de 1 a 16 años, situación que fortalece la seguridad del ciberespacio, manteniendo así normativas urgentes de acuerdo a las necesidades actuales del siglo XXI.

Palabras Claves: Delitos informáticos, COIP, tecnología, jurídico, ilícito, ciberespacio.

1. INTRODUCCIÓN

La tecnología ha generado grandes cambios en la sociedad, es en pleno siglo XXI donde las transformaciones políticas, sociales, culturales, financieras significan aporte concreto en las actividades rutinarias del ser humano. Con el paso de tiempo las transacciones bancarias, trámites burocráticos a nivel nacional e internacional se realizan a través de medios electrónicos, por lo que la informática constituye el sector más dinámico de la economía mundial. Sin embargo esto ha traído consigo también la evolución en el cometimiento de delitos, posibilidades de delincuencia antes impensables. Existe una inmensa cantidad de información en los servidores informáticos gubernamentales, financieros y empresariales; información que es susceptible de ser alterada o usada en forma fraudulenta, la misma que genera interés de tipo económico, político y/o social. Esta se ha constituido en una nueva forma de delinquir denominada “delito informático”, a su vez esto no requiere grandes medios económicos ni tecnológicos, sino que depende de la astucia de los llamados hackers informáticos o personas especialistas en software, ya que es suficiente tener acceso a un teclado alfanumérico, acceso a internet y conocimiento del procesamiento electrónico de datos como únicas herramientas que necesita el delincuente para provocar grandes perjuicios morales, económicos y hasta materiales a causa de la divulgación inescrupulosa de información privilegiada; la cuantía de daños de este tipo de delitos puede ser mucho mayor a lo provocado por la delincuencia tradicional.

De acuerdo al informe de Norton sobre delitos informáticos elaborado en el 2012, “los costos asociados con los delitos informáticos en el mundo ascendieron a US$ 110.000 billones anuales” (Norton, 2013). Ante esta creciente modalidad de actos ilícitos, que aumenta la vulnerabilidad de una sociedad globalizada, se vuelve imperiosa la necesidad de tener una marco legal que abarque de manera integral este tipo de delitos

En virtud de ello, se analizará la normativa legal vigente ecuatoriana respecto a los delitos informáticos que se encuentran tipificados en el Código Orgánico Integral Penal, y se realiza la comparación con la normativa de otros países, para conocer sobre la existencia de otros delitos informáticos que se pudieran estar presentando y que al no haber sido incorporados en nuestra legislación podrían estar cayendo en un vacío legal.

Es importante contar con un sistema jurídico que ofrezca confianza a los usuarios y para ello se hace un análisis de nuestra realidad nacional en cuanto a la aplicación de la normativa legal vigente y el debido proceso, respecto a los delitos informáticos, con la idea de concientizar al lector sobre la importancia de mantener herramientas de protección de la información de tal forma que se prevenga de cierta forma algún tipo de delito informático, aun cuando otros son totalmente impredecibles.

El presente documento pretende ser un aporte legal y social. Dada la importancia de la tecnología en el día a día de los individuos y al estar presente en casi todos los ámbitos de nuestras vidas la legislación debe aportar con regulaciones específicas y leyes que estén acorde a la realidad en la que vivimos, para que el cometimiento de cualquier tipo de delito informático sea penado y que la sociedad tenga claro conocimiento de todo lo que se puede constituir en este tipo de ilícitos.

2. DESARROLLO

2.1. DEFINICIONES

Es necesario iniciar con el análisis del tratamiento que se le da en Ecuador a los delitos informáticos, para lo cual se requiere conocer su definición para ubicarlos en la rama de Derecho que corresponde, por lo que es importante delimitar también el significado de los términos Informático y la Informática Jurídica.

2.1.1. DELITO INFORMÁTICO

Se denomina delito informático “a una nueva tendencia para la comisión de delitos en la sociedad, es decir el empleo de la informática con ánimo doloso o culposo” (Iriarte, 2005), es decir que dentro del derecho el delito informático se plasma como un delito que puede ser tanto culposo como doloso.

A su vez, se detalla que:

> Un delito informático o ciberdelito, es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas, que también se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encontrar las nuevas formas delictivas. (Correa, Batto, Caza, & Nazar, 2013)

En mayo de 1983, “la Organización de Cooperación y Desarrollo Económico – OCDE, reunida en Francia definió Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos." (Ycaza, 1983)

Para Julio Téllez Valdésos los delitos informáticos representan "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto

atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico). (Valdésos, 2008)
Dentro del Código Orgánico Integral Penal se encuentra tipificado en el uso de un sistema informático o redes electrónicas y de telecomunicaciones se genera la apropiación de un bien ajeno o aquel que se establece como “la transferencia no consentida de bienes, valores o derechos que se otorgan en perjuicio de esta persona o una tercera en función de redes electrónicas, programas, sistemas informáticos, equipos terminales” (Código Orgánico Integral Penal, 2014). Con lo dicho anteriormente es posible visualizar a simple vista que al hablar de robo informático se trata de una actividad totalmente de carácter ilegal incluso mucho más exhaustiva que en el caso de cualquier otro bien.

2.1.2. EL DERECHO INFORMÁTICO

Dado que el delito informático está compuesto por diferentes características, no es posible aplicar protección legal tradicional, por ello el Derecho debe ser modificado y ampliado con la celeridad con la que la tecnología tiende a transformarse, para responder eficientemente a los problemas que surgen en el entorno tecnológico y en general a nivel social con respecto a esta temática.

Se habla del Derecho Informático como “una rama del Derecho que permite ortogar las soluciones jurídicas adecuadas a los problemas originados por el uso de las tecnologías, en las diversas actividades del ser humano.” (Cepeda, 2005), es decir que, este tipo de derecho es una rama de la jurisprudencia general de una nación, por ende ha de cumplir a cabalidad con sus principios normativos y de carácter constitucional, para este caso constituido por la garantía de la seguridad de la información.

El Dr. Juan José Ríos Estavillo, define al Derecho Informático como: “una ciencia jurídica encaminada al estudio de las normas jurídicas que regulan el mundo informático, su objetivo principal es lograr la regulación del universo informático; estudia la doctrina y jurisprudencia que se origine como consecuencia del uso de la informática” (Estavillo, 2005), lo anterior

citado define al derecho informático como aquella necesidad de instaurar normas permisibles y las sanciones con respecto al uso y abuso de la información virtual.

2.2. TIPOS DE DELITOS INFORMÁTICOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL

En el Ecuador, el 10 de agosto de 2014 se expidió el Código Orgánico Penal Integral – COIP, en el que se establecen los delitos en el área informática de forma independiente y autónoma, en diferentes secciones. En torno a este cuerpo legal, se derogó al Código Penal vigente desde el año 2002, así como a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos misma que brindó cierta seguridad jurídica a las relaciones vinculadas con la tecnología, y dio paso a reformar en el Código Penal de ese entonces para incluir los llamados delitos informáticos dentro del nuevo COIP.

En los siguientes artículos del Libro Primero “La Infracción Penal” del Código Orgánico Integral Penal se encuentran normandos los delitos informáticos:

- Revelación ilegal de base de datos: Artículo 229

  Se refiere a la violación de información confidencial que se encuentra en una base de datos u otro similar, la pena es de uno a tres años. Sin embargo es un agravante que el delito sea cometido por un servidor público o colaboradores de instituciones bancarias que realicen intermediación financiera o contratistas, en estos casos el delito se sanciona con pena privativa de libertad de tres a cinco años. (Código Orgánico Integral Penal, 2014)

- Interceptación ilegal de datos: Artículo 230

  La llamada interceptación ilegal

  Cuando sin orden judicial previa, se intercepta, un dato informático, una señal o una transmisión de datos o señales con el fin de obtener esta información registrada. Este delito se sanciona con pena privativa de libertad de tres a cinco años. (Código Orgánico Integral Penal, 2014)

Este artículo permite también sancionar la clonación de tarjetas de débito y crédito, así como también el desarrollo de software malicioso, envío de mensajes o realización de llamadas que induzcan a ingresar a una dirección o sitio de web diferente a la que quiere acceder ya sea este un servicio financiero, pago electrónico o cualquier otro sitio personal o de confianza.

- Transferencia electrónica de activo patrimonial: Artículo 231

  Con pena privativa de libertad de tres a cinco años se sanciona la alteración o manipulación de un activo patrimonial de manera no consentida.
- Ataque a la integridad de sistemas informáticos: Artículo 232

  Se refiere a la acción que ocasione destrucción, alteración o mal funcionamiento de sistemas de tratamiento de información, telemático o de telecomunicaciones.

  En cuanto a este delito se habla de “sanciones con penas privativas de tres a cinco años, y para casos donde se realice este delito a bienes informáticos como parte de una prestación de servicio público o con vínculo con la sociedad sería un total de cinco a siete años de privación de libertad” (Código Orgánico Integral Penal, 2014)

  Esta situación se hace evidente a medida que se han implementado nuevas penas y sanciones para limitar a quienes hacen de la información un negocio ilegal.
- Delitos contra la información pública reservada legalmente: Artículo 233

  Se habla de “quien destruya o inutilice información pública clasificada de conformidad con la Ley será sancionado con pena de tres a cinco años” (Código Orgánico Integral Penal, 2014), en el país hay información que también es pública la cual está autorizada para ser divulgada, en base a los principios de publicidad, la misma que no se tipifica como delito alguno por tener el derecho a su divulgación.

- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: Artículo 234

  Este delito sanciona a la persona o conjunto de personas que accedan ilegítimamente, es decir sin autorización, a un portal web, o que redireccionen el tráfico de datos o voz a fin de lucrarse ilícitamente de esta acción u ofrecer servicios que estos sistemas provean a terceros.

En el art. 190 del COIP, se habla acerca de la apropiación fraudulenta por medios de tipo electrónico, en donde se hace énfasis en el artículo 190 en la apropiación fraudulenta por medios electrónicos "son aquellos donde se realiza un fraude a un sistema informático o redes electrónicas y de telecomunicación con el fin de apropiarse de un bien ajeno o la transferencia no consentida tanto de bienes como valores o derechos en perjuicio de la persona o un tercero" (Código Orgánico Integral Penal, 2014), en este ámbito se hace referencia a la gran necesidad de salvaguardar los bienes y valores por ejemplo en el caso de cuentas bancarias, donde es posible intervenir también de forma virtual, lo cual ya se considera un delito con pena privativa de libertad de hasta tres años.

Existen otros delitos tipificados en el COIP que pueden ser relacionados con delitos informáticos, tales como:

El artículo 103 que habla sobre "pornografía con utilización de niñas, niños o adolescentes, donde queda tipificado el delito de aquella persona que realice fotografías, grabaciones, transmisiones, edición de materiales visuales, informáticos, electrónicos y de otro tipo de soporte con contenido desnudos o semidesnudos o simulando actitudes sexuales" (Código Orgánico Integral Penal, 2014), es así como se hace evidente la importancia de anclar cada vez nuevas normativas legales y penales para limitar este tipo de delitos totalmente que atentan contra la calidad de vida de una persona o de un menor de edad.

A su vez existe el artículo 173 del COIP que habla sobre el contacto con la finalidad sexual con menores de dieciocho años por medios electrónicos

que establece que “la persona que por algún medio virtual proponga encuentros con personas menores de dieciocho años con propuestas de actos con finalidad sexual o erótica será sancionada con penas privativas de hasta tres años” (Código Orgánico Integral Penal, 2014), también “la persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.” (Código Orgánico Integral Penal, 2014)

El castigo es de 3 a 5 años cuando el acercamiento se obtenga mediante coacción o intimidación, al igual que cuando se suplante la identidad de un tercero o mediante el uso de un usuario falso y se establezca comunicaciones de contenido sexual o erótico.

Dentro del artículo 174 del COIP también se establece una norma acerca de la oferta de servicios sexuales con menores de dieciocho años por medios electrónicos que indica:

> La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años. (Código Orgánico Integral Penal, 2014)

Será sancionada con pena privativa de libertad de 7 a 10 años, a quien por medios electrónicos ofrezca servicios sexuales con menores de 18 años, lo cual se plantea como un delito agravante.

Para estos delitos tipificados en el art. 173 y 174 del COIP buscan prevenir no solo el cometimiento de delitos informáticos sino también la pornografía infantil, por lo que se vuelve necesaria la existencia de convenios de cooperación internacional que permiten que estas leyes

sean más eficientes, puesto que las redes de pornografía infantil operan de manera simultánea desde diferentes países.

Sin embargo, es importante mencionar que el artículo 174 eliminó el vacío legal, que existía en el anterior código penal, en el que únicamente se sancionaba a quienes cometían un delito sexual más no a quienes lo ofrecían.

A su vez existe el artículo 178 sobre la Violación a la intimidad, el mismo que establece que "la persona que, sin contar con el debido consentimiento o la autorización legal, acceda de una u otra forma a publicación de datos personales, mensajes de voz, audio y video, así como otra información, será sancionada con pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014), es decir que, también es un delito atentar contra la intimidad de una persona y divulgar información confidencial de ella.

Este artículo tipifica y sanciona la grabación y/o difusión mediática de videos, mensajes, textos, audios y fotografías que contengan aspectos sensibles y sobre los que no se ha consentido que se ha conocidos por terceros.

Este tipo de casos se han dado con frecuencia, en nuestro país, algunos han sido de conocimiento nacional como por ejemplo, la difusión de fotografías íntimas de Mery Zamora (ex dirigente política) mediante la red social twitter. Sin embargo, este tipo de delitos no suelen ser denunciados, quizás por desconocimiento de la norma, o porque –como en el caso de Mary Zamora- son realizados desde el anonimato, y al no contar el Ecuador con cruce de datos informáticos se complica detectar las cuentas o las direcciones IP desde las que se realiza la violación; ya que los bancos de datos de usuarios de redes sociales se encuentran en Estados Unidos y obtener la información puede tardar varios meses.

En torno al artículo 186 se habla de la estafa como aquella donde:

> La persona, que para obtener un beneficio patrimonial para sí misma o para una tercera persona, por medio de la simulación de hechos falsos o la deformación de hechos verdaderos, y alguna otra que induzca a error, con el fin de perjudicar su patrimonio o de un tercero será sancionado con pena privativa de libertad de cinco a siete años. (Código Orgánico Integral Penal, 2014)

Es así como, la estafa también es sancionada pues esta asume la condici´{on de un hecho con el objeto de obtener beneficios para una persona o un tercero con engaños previos que afectan a la víctima, lo cual es aplicable con pena privativa de libertad de hasta siete años, en torno a que sus dispositivos pueden ser alterados, clonados o modificados, como el caso de una tarjeta de crédito o débito.

A partir del artículo 191 hasta el 195 del COIP se encuentran tipificados los delitos cometidos con la utilización de terminales móviles, pues hoy por hoy el uso de la tecnología móvil es una de las más difundidas en la ciudadanía, por ello se establece el artículo 191 que habla sobre la reprogramación o modificación de información de equipos terminales móviles, el cual detalla que “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.” (Código Orgánico Integral Penal, 2014).

En lo que refiere a esta es de uno a tres años, en lo que tiene que ver con modificación de información de identidad de equipos terminales, o dispositivos móviles, de tal manera que estos están registrados en la plataforma tecnológica de la Superitendencia de Telecomunicaciones, lo cual a su vez forma parte de la contribución para prevenir robos o contrabando.

En lo que se refiere al artículo 192 del COIP se detalla sobre el intercambio de la información, su comercialización, compra de información de equipos terminales móviles, es así que “la persona que intercambie, o realiza la comercialización de bases de datos que disponen de contenidos de

identificación de equipos terminales móviles, serán sancionados con pena de privación de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014).

En el artículo 193 también se habla del reemplazo de identificación de terminales móviles es decir que "aquellas personas que reemplacen las etiquetas de fábrica de las terminales móviles que contengan información de identidad de estos equipos y en su lugar coloquen otra etiquetas con información de identificación falsa o distinta a la original, tiene pena privativa de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014), en lo referente a los siguientes artículos como son el artículo 194, habla sobre la comercialización ilícita de las terminales móviles, donde se indic que "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" (Código Orgánico Integral Penal, 2014).

Así también existen otros artículos con referencia a la divulgación de información tanto física como virtual y las respectiva sanciones, tal como es el caso del artículo 195, el cual narra sobre la infraestructura ilícita, es aquella donde "la persona que tiene infraestructura, equipos, bases, programas, etiquetas, que tienen la opción de reprogramar, modificar o alterar información de identidad de un equipo terminal móvil será sancionado con privación de libertad de uno a tres años" (Código Orgánico Integral Penal, 2014), tal como se puede observar, es posible entender que, la mayoría de normativas en torno a delitos de información que no se trate de situaciones de tipo sexual disponen de penas entre uno a tres años de privación de la libertad.

La tipificación este tipo de delitos en el Código Orgánico Integral Penal Ecuatoriano ha permitido sancionar los actos ilícitos con penas privativas de libertad para diferentes actores de la seguridad informática, y como se ha

citado anteriormente ha permitido llenar ciertos vacíos legales existentes en las normativas previas al Código Orgánico Integral Penal.

2.3. DERECHO COMPARADO EN RELACIÓN A LOS DELITOS INFORMÁTICOS

En torno a lo dicho por la Organización de Naciones Unidas, se reconocen actualmente tres tipos de delitos informáticos como son “los fraudes cometidos por manipulación de computadoras, la manipulación de datos de entrada, los daños o modificaciones de programas o datos computarizados”, es así que, existen legislaciones de distintos países que tienen como propósito la protección de los sistemas informáticos que utilizan, con el fin de sancionar los delitos cometidos a causa de este tipo de delitos.

Son pocos los países que en la actualidad cuentan con normativas idóneas en cuanto a tipificación y sanción de delitos informáticos, sin embargo solo en países como Argentina , Uruguay y Colombia en el caso de América Latina se han definido sanciones ejecutoriadas para el caso de delitos informáticos.

Para el presente análisis se ha considerado las legislaciones de Chile y Argentina, por tratarse de naciones con similares coyunturas sociales lo que permite comparar las realidades y tendencias, puesto que ambos son países latinos que han sido considerados ya como países emergentes y ya no en vías de desarrollo, pues han sabido salir adelante a pesar de sus restricciones políticas principalmente en cuanto a regímenes dictatoriales, los que han sido un limitante en ciertos tiempos para que la revolución tecnológica se posicione en ellos a la par que el resto de países del mundo, sin embargo, gracias a su gestión interna y su avance empresarial, hoy por hoy se han sabido posicionar en el campo tecnológico con mayor relevancia, producto de esto los gobiernos han visto necesaria la implementación de nuevas y cada vez más variadas formas de proteger la información privilegiada del ciberespacio y sancionar delitos en contra de esta o de la integridad de personas.

2.3.1. CÓDIGO PENAL CHILENO

Chile fue el primer país de latinoamericano que estableció en su normativa penal las sanciones para los delitos informáticos. La pena mínima, por el cometimiento de este tipo de delitos es de tres años.

Tres leyes norman en Chile estos delitos: Ley N° 17.336, abarca delitos relativos a la Propiedad Intelectual, Ley N° 19.223 encontramos tipos penales relacionadas a la informática; y la Ley N° 19.927 relativa a cambios efectuados en temas de pornografía infantil.

En 1993 fue posible la proclamación y vigencia de la Ley N. 19223, fue así como este país se convirtió en el pionero en torno a la temática de normas sancionadoras con respecto a delitos informáticos.

LEY RELATIVA A DELITOS INFORMATICOS - Ley No. 19223 Año 1993.

En el artículo 1 de la Ley Relativa a Delitos Informáticos se habla de que “aquella persona que destruya o inutilice de manera maliciosa, un sistema de tratamiento de información o sus partes sufrirá de penas de presidio menor en su grado medio a máximo” (Ley Relativa a Delitos Informáticos, 1993), se plantea también como consecuencia en el caso de que se impida, se cree obstáculos o se modifique su funcionamiento, sufrirá penas de privación de la libertad considerada como pena de presidio menor en su medio a máximo.

Es así como se puede relacionar esta Ley con respecto a lo estipulado en el Ecuador en el COIP, donde se hace paso a un tratamiento de penas hasta tres años cuando se gestionan conductas maliciosas sobre la información privilegiada haciendo daño a una persona o información de carácter público.

En lo que respecta al artículo 2 se habla sobre “El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio” (Ley Relativa a Delitos Informáticos, 1993), en Chile desde los años 90 se

consideró ya a la divulgación indebida de la información como un delito, incluyendo interceptaciones e interferencias y también está catalogada como delito menor en su grado mínimo a medio.

“Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.” (Ley Relativa a Delitos Informáticos, 1993).

Este artículo sanciona con presidio, que puede ser desde 541 días hasta 3 años a quien dañe el contenido de un equipo o sistema informático, como por ejemplo instalar algún virus en un sistema, es decir que, en Chile hay mucha más rigurosidad en temas de delitos informáticos, pues este artículo no se lo contempla en el caso del Ecuador.

“Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado." (Ley Relativa a Delitos Informáticos, 1993), es así como se hace énfasis en la revelación o difusión de datos que han de afectar a la persona o terceros, pues en el caso de que así fuera se considera una pena menor en su grado medio pero cuando esto lo hace la misma persona que se ha responsabilizado del sistema informático la pena aumentará con pena de grado medio a grave.

Quien revele el contenido de la información que se encuentre en un sistema informático será sancionado con prisión desde 541 días hasta 3 años, esta pena podría aumentar a 5 años si quien cometió el delito es el responsable de operar el sistema.

Los artículos 1 y 3 de la Ley Nº 19.223, re refieren al sabotaje informático; mientras que los artículos 2 y 4 de la misma Ley tipifican el espionaje informático

En cuanto a los castigos señalados en los artículos de esta Ley, y según González: es importante precisar que para estos delitos la ley establece penas de presidio menor diferentes grados que van de mínimo, medio o máximo, por lo que dependiendo de la gravedad del delito cometido el juzgador podrá aplicar penas privativas de libertad que van desde los 61 días a 5 años. (González, 2015), esta situación se ejecuta debido a que no se puede catalogar a todos los delitos cibernéticos con la misma magnitud, pues depende del daño o agravante que haya cometido o si estos se encuentran anexos a otros delitos, como es el caso de estafas o delitos de divulgación u oferta sexual.

En abril de 2017 a fin de mejorar las falencias que existían en la ley N° 19.223 y fortalecer la política de seguridad informática, se remitió al congreso nuevos delitos para ser agregados, esto lo hicieron con el fin de incluir en la misma ley aquellas necesidades que se van generando con la transformación del medio social y tecnológico de la época, entendiendo que cada vez la tecnología evoluciona así también se han buscado nuevos medios de desviación de información o de otros delitos de divulgación de la misma a nivel cibernético, entre los que se encuentran:

- Captación visual y sonora de información sin consentimiento
- Difusión de ese material
- Producción de programas o dispositivos para cometer delitos
- Difusión de información de un sistema informático
- Manipulación de claves confidenciales y de datos codificados en una tarjeta
- Uso de programas o dispositivos para vulnerar la integridad de datos
- Alteración o daño de sistemas informáticos
- Alteración de datos para acceder a un sistema informático

2.3.2. CÓDIGO PENAL ARGENTINO

No fue sino hasta junio de 2008 que la Cámara de Senadores del Congreso Nacional decidió aprobar la Ley 26.388 en la que se penalizan los delitos electrónicos y tecnológicos en Argentina. Antes no existía la tipificación delitos informáticos como tales, sin embargo el 4 de octubre del 2000 entró

en vigencia la Ley 25.326 de PROTECCIÓN DE LOS DATOS PERSONALES, que se caracterizaba por la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados.

Adicionalmente, la Ley 11.723 de REGIMEN LEGAL DE LA PROPIEDAD INTELECTUAL sancionada el 28 de septiembre de 1933, y su posterior modificación: Propiedad intelectual, Ley 25036 que modifica los artículos 1º, 4º, 9º y 57º e incorpora el artículo 55 bis a la Ley 11723 regula la propiedad intelectual, sobre obras científicas, literarias y artísticas, y comprende los "escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto".

La Ley 26.388 establece que: El "objeto material" de todo delito es la entidad, persona o cosa sobre que recae la conducta reprochable penalmente, en lo que hace referencia al fraude informático en su artículo 173 en el inciso 16 CP, se habla de su concepción como aquella acción que "consiste en defraudar por medio de cualquier técnica de manipulación informática que altere el funcionamiento normal de cualquier sistema informático o de transmisión de datos" (Ley 26.388, 2008), esta ley complementa a la ley 19.223, entendiendo como delito aquel fraude a nivel informático.

Se habla también de daño o sabotaje a nivel informático, en contemplación con los artículos 183 y 184, en los incisos 5 y 6 CP, en los cuales se habla de "la alteración, destrucción, inutilización de datos, documentos o de cualquier otro tipo de programa de tipo informático que cause daños" (Ley 26.388, 2008) es así que, los datos establecidos en este inciso habla por ejemplo de algún daño por medio de un virus cibernético u otro medio que sabotee datos o los dañe.

Existen también otros delitos informáticos que se han definido en torno a las irregularidades que se atraviesa en la actualidad, como son la pornografía infantil establecida en el artículo 128 CP, la violación, apoderamiento y

desvío de comunicación electrónicos en el artículo 153 en el párrafo primero del CP, y la publicación de una comunicación electrónica, correspondiente al artículo 155 CP, así como la intercepción o la captación de comunicaciones electrónicas o telecomunicaciones, para artículo 153, párrafo 2° CP, acceso a un sistema o dato informático según el artículo 153 CP, así como la revelación de la información que se registra en un banco de datos personales existente en el artículo 157 del párrafo 2°CP.

2.4. REALIDAD PROCESAL EN EL ECUADOR RESPECTO A DELITOS INFORMÁTICOS

Según datos recopilados por la Fiscalía General del Estado –FGE, expuestos en un boletín publicado el 13 de junio del 2015, los delitos más comunes son: Transferencia ilícita de dinero, apropiación fraudulenta de datos personales, interceptación ilegal de datos, acoso sexual, se ha creado la Unidad de Criminalística como unidad de delitos y en especial de tipo sexual, donde también intervienen pruebas basadas en datos informáticos.

Fue así que, se instauró el COIP desde el 10 de agosto del 2014, y se tiene el dato de que “solo hasta Mayo del 2015 la Fiscalía General del Estado registró 626 denuncias por delitos informáticos” (Código Orgánico Integral Penal, 2014). Y, durante los primeros cinco meses del 2016 la FGE registró 530 delitos informáticos, una aparente disminución, a pesar de que se conoce que el 80% de los delitos informáticos no son reportados, es decir existe lo que podríamos denominar la falta de una cultura de denuncia. Estos delitos no son atendidos por unidad especializada en delitos informáticos. Actualmente, cuando es necesario se oficia a la Unidad de Criminalística Forense realizar el peritaje que determine la existencia de este tipo de ilícitos.

Este desconocimiento resulta en la falta de confianza de parte de los afectados hacia el sistema judicial, y en el caso de los operadores de justicia la complicación al investigar este tipo de delitos. Criterio que ha sido expuesto en el análisis efectuado por el abogado e ingeniero en sistemas.

Erwin Chiluiza quien expresa que:

> A pesar de contar con la normativa que permite sancionar el cometimiento de delitos informáticos, existe falta de entendimiento de la aplicación de la ley en cuanto a los ilícitos llevados a cabo mediante herramientas electrónicos e informáticas, de nada serviría la nueva normativa, y considera que uno de los principales inconvenientes en torno al delito informático es la obtención de la prueba, dada la falta de conocimiento y herramientas para obtenerlas en un proceso. (Chiluiza, 2014)

La aseveración anterior se fundamenta en que, debido a las denuncias que inician por presunción de otros ilícitos (robo, estafa, etc.) es como suelen desarrollarse las investigaciones a nivel informático, es decir "inician como un delito común y en el desarrollo de la investigación se llevan a cabo diligencias a nivel informático" (Chiluiza, 2014). Por ello estas investigaciones tienden a ser llevadas por organismos auxiliares ajenos a expertos informáticos, como la de Daños contra la Propiedad, de Delitos Financieros, entre otros; esto es lo que resulta de la falta de un grupo especializado que opere específicamente los delitos informáticos, esto se corrobora también con la actuación de la Unidad De Criminalística para el caso del Ecuador.

Es importante que quienes participen en el proceso del juzgamiento del delito informático tengan la preparación necesaria que asegure el adecuado desarrollo del proceso, pues muchas veces se encuentran confundidos ante el tratamiento de este tipo de delitos y los términos relacionados a éste, lo que dificulta dar siempre el tratamiento jurídico que estos delitos merecen. Según el análisis efectuado por el autor Arroyo Jácome se incluye encuesta realizada a 10 jueces y respecto a la pregunta ""¿Es suficiente el dominio de los operadores del Derecho sobre los Delitos Informáticos?" el 60% respondió que no, frente al 40% que manifestó que sí es suficiente". (Jácome, 2013)

Cabe destacar que, el Ecuador no cuenta con convenios internacionales respecto a delitos informáticos. Se debe tipificar en consenso todos los delitos informáticos que se cometen en diferentes partes del mundo, así podría realizarse la equiparación de estos a nivel internacional a través de tratados internacionales que permitan actuar efectivamente. Esto significaría el desarrollo de un sistema jurídico internacional que garantice la adecuada aplicación de la normativa existente en cada país. Al respecto en el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal señala que la cooperación internacional se ve facilitada cuando en los marcos jurídicos nacionales se tipifican como delito las mismas conductas.

3. CONCLUSIONES

Cabe destacar que, la función del ordenamiento jurídico no debe limitarse únicamente a asegurar las condiciones fundamentales de la vida, sino también a promover el desarrollo y mejoramiento de la sociedad. Los primeros pasos, respecto al cometimiento de delitos relacionados a las nuevas tecnologías, están dados en nuestro país, con la inclusión de estos en el COIP, sin embargo es necesario fortalecer el sistema con personal especializado en delito informático.

Si bien los delitos informáticos son obra, por lo general, de personas aisladas, también intervienen en ellos grupos delictivos organizados. Este elemento es especialmente importante, porque abre la posibilidad de aplicar instrumentos concebidos para promover la cooperación para prevenir y combatir la delincuencia organizada transnacional, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, en cuyo artículo 29 de Capacitación y asistencia técnica, literal h) señala que los Estados Parte desarrollará o perfeccionará programas concebidos para el personal encargado de hacer cumplir la ley los mismos que guardarán relación con "Los métodos utilizados para combatir la delincuencia organizada transnacional mediante computadoras, redes de telecomunicaciones u otras formas de la tecnología moderna." (Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, 2014)

Respecto a la delincuencia organizada transnacional, y dado que los delitos informáticos suelen incluso suscitarse desde un país diferente al que se encuentra la víctima, es conveniente sujetarse a un convenio internacional en donde se aplique entre otros el principio de la universalidad y justicia mundial, es decir se aplica la ley del país haya detenido primero al delincuente, esto permitirá actuar de manera efectiva siempre se tipifique de manera clara e integral todo tipo de delitos informáticos.

4. REFERENCIAS

Cepeda. (2005). *Derecho informático y seguridad jurídica.* Barcelona.

Chiluiza, M. (2014). *Delitos del ciberespacio.* Madrid.

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal.* Quito.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. (2014). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.* Quito.

Correa, C., Batto, H., Caza, S., & Nazar, E. (2013). *El derecho ante el desafío de la Informática.* Argentina.

Estavillo, J. J. (2005). *El derecho informático.*

González, A. (2015). *Presidio Menor en Chile*. Obtenido de https://chile.leyderecho.org/presidio-menor/

Iriarte Ahon, E. (2005). *Sociedad de la información: Políticas y Regulación en América Latina y el Caribe ¿Hacia dónde vamos los.*

Jácome, A. (2013). *Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. .* Quito: Universidad Central del Ecuador.

Ley 26.388. (2008). *Ley 26.388.* Santiago de Chile.

Ley Relativa a Delitos Informáticos. (1993). *Ley N.19223.* Santiago de Chile.

Norton. (2013). *Reporte Norton 2013*. Obtenido de https://www.symantec.com/content/es/mx/about/presskits/b-norton-report-2013-final-report-lam-es-mx.pdf

Valdésos, J. T. (2008). *Los delitos informáticos.* Madrid.

Ycaza, A. (1983). *¿Cuándo y dónde lo definió así?* Francia: Colocado.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Espinoza Jurado Sindy Fernanda** con C.C: # 0926690959 autor/a del trabajo de titulación: **Tratamiento jurídico de los delitos informáticos en el Ecuador,** previo a la obtención del título de **Abogada de los Tribunales y Juzgados de la República del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 23 de febrero del 2019

f. _____

Nombre: **Espinoza Jurado Sindy Fernanda**

C.C: **0926690959**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	Tratamiento jurídico de los delitos informáticos en el ecuador.		
AUTOR(ES)	Sindy Fernanda Espinoza Jurado		
REVISOR(ES)/TUTOR(ES)	Ab. Ycaza Mantilla Andrés Patricio, Mgs		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia y Ciencias Sociales y Politicas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogada de los tribunales y juzgados de la República del Ecuador		
FECHA DE PUBLICACIÓN:	23 de febrero del 2019	**No. DE PÁGINAS:**	22
ÁREAS TEMÁTICAS:	Civil, Penal		
PALABRAS CLAVES/ KEYWORDS:	Delitos informáticos, COIP, tecnología, jurídico, ilícito, ciberespacio.		

RESUMEN/ABSTRACT:
El presente ensayo tiene como propósito el análisis sobre el tratamiento jurídico de los nuevos delitos que han surgido en los últimos años conjuntamente con la evolución de la tecnología denominados delitos informáticos; los cuales pueden ser cometidos en tiempo real, utilizando únicamente un equipo informático y sin estar presente físicamente en el lugar de los hechos.
En nuestro país el Código Orgánico Penal Integral – COIP, establece los delitos en el área informática de forma independiente y autónoma, en diferentes secciones. La tipificación este tipo de delitos en el Código Orgánico Integral Penal Ecuatoriano ha permitido sancionar los actos ilícitos con penas privativas de libertad para diferentes actores de la seguridad informática, que van de 1 a 16 años, situación que fortalece la seguridad del ciberespacio, manteniendo así normativas urgentes de acuerdo a las necesidades actuales del siglo XXI.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-4-993225006	E-mail: **sifeespi@gmail.com**
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	Nombre: Toscanini Sequeira, Paola. Ab. Mgs.	
	Teléfono: +593-42206950	
	E-mail: paolats77@hotmail.com	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	