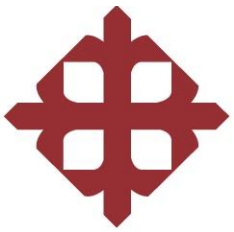


UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

Los delitos informáticos y su afectación sobre los bienes jurídicos

AUTOR:

Jorge Adrián Hidalgo Pazmiño

Trabajo de Titulación previo a la obtención del título

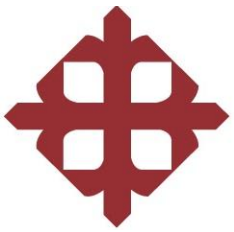
ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPÙBLICA

TUTOR:

Ab. Edgar Escobar Zambrano, Mgs.

Guayaquil - ECUADOR

22 de febrero del 2018



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 **Jorge Adrián Hidalgo Pazmiño**, como requerimiento para la obtención del Título de Abogado de los Tribunales y Juzgados de la República.

TUTOR (A)

f. _____

Ab. Edgar Escobar Zambrano, Mgs.

DIRECTOR DE LA CARRERA

f. _____

Ab. Lynch de Nath María Isabel, Mgs.

Guayaquil, a los 22 días del mes de febrero del año 2018.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, Jorge Adrián Hidalgo Pazmiño.

DECLARO QUE:

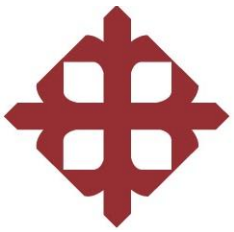
El trabajo de Titulación "Los delitos informáticos y su afectación sobre los bienes jurídicos", previo a la obtención del Título de Abogado de los Tribunales y Juzgados de la República, ha sido desarrollado respetando derechos intelectuales de terceros, conforme a las citas que en éste documento constan, cuyas fuentes se incorporan en las referencias o bibliografía. Consecuentemente este trabajo es de mi total autoría.

Guayaquil, a los 22 días del mes de febrero del año 2018.

EL AUTOR (A)

f._____

Jorge Adrián Hidalgo Pazmiño



UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, Jorge Adrián Hidalgo Pazmiño

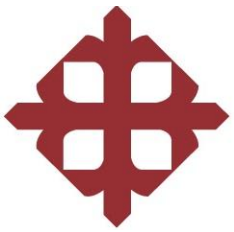
Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la Institución del trabajo de Titulación "Análisis Jurídico de los obligados principales y obligados subsidiarios en materia de alimentos", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 22 días del mes de febrero del año 2018.

EL AUTOR:

f._____

Jorge Adrián Hidalgo Pazmiño



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.

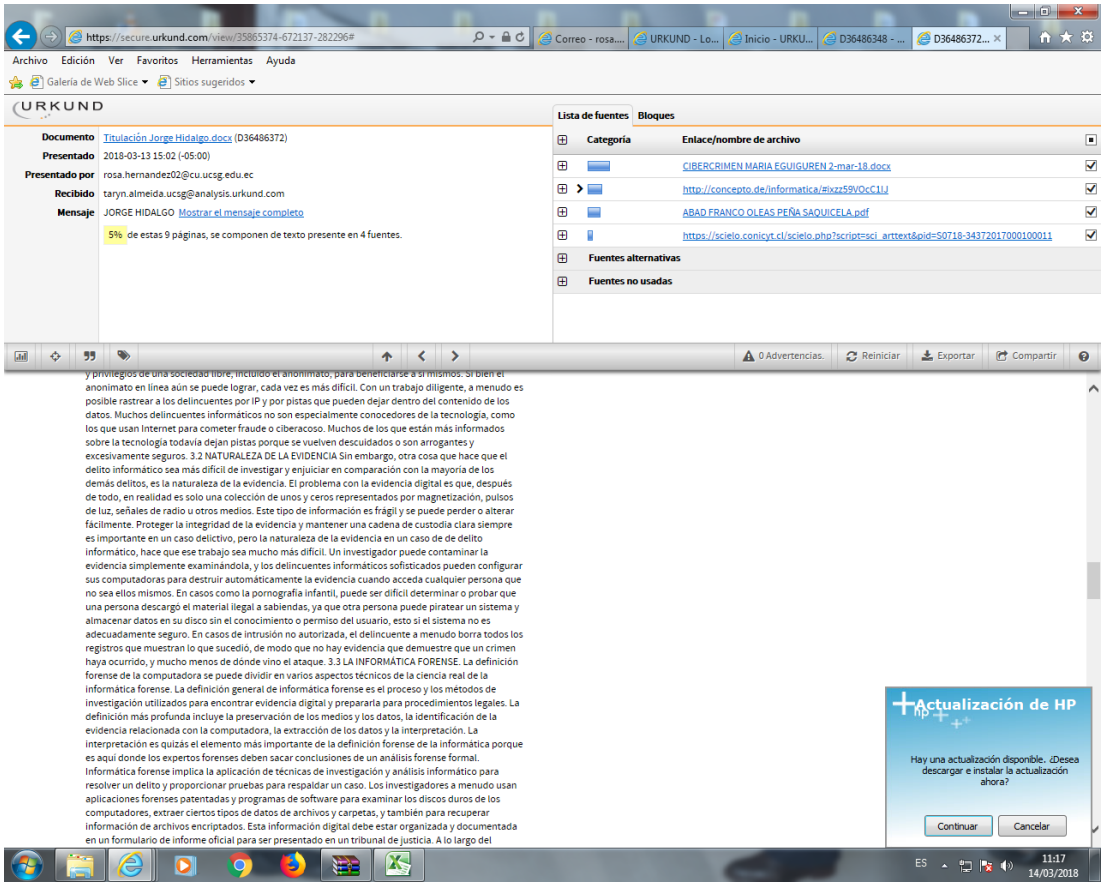
COORDINADORA DEL ÁREA

f. _____

Ab. Roxana Gómez Villavicencio, Mgs.

OPONENTE

REPORTE URKUND



EL AUTOR:

f._____

Jorge Adrián Hidalgo Pazmiño

TUTOR (A)

f. _____

Dr. Zambrano Veintimilla Carlos Luis. Mgs.

INDICE

DEDICATORIA.

Este trabajo está dedicado a mis padres quienes han sido el soporte fundamental en cada una de las decisiones que he tomado a lo largo de los años. Está dedicado en especial a mi madre, la Sra. Martha Pazmiño Morales, quien, con su cariño, ejemplo, consejo y apoyo incondicional, se ha convertido en el pilar esencial en cada meta que he conseguido alcanzar.

RESUMEN

En los últimos años, Internet ha crecido explosivamente. En comparación con los 26 millones de usuarios enumerados en 1995, hoy en día más de 200 millones de personas se comunican, compran, pagan facturas, comercian e incluso consultan a su médico en Internet.

Mientras Internet estaba en auge, el crimen en línea también estaba creciendo. Los delincuentes informáticos, como se los llama, han invadido o invadido en gran medida el mundo virtual, cometiendo delitos tales como el uso de códigos de acceso confidenciales, piratería informática, fraude, sabotaje informático, tráfico de drogas, pornografía pedófila y "acoso cibernético".

Los delincuentes informáticos son tan variados como las diferentes formas de delincuencia que practican. Pueden ser estudiantes, terroristas o criminales organizado. Los delincuentes informáticos pueden cruzar las fronteras a un ritmo rápido, pasar desapercibidos, ocultos detrás de innumerables "enlaces" o simplemente desaparecer sin dejar rastro. Pueden pasar las comunicaciones a través de "paraísos de datos" u ocultar la evidencia de sus delitos.

1. INTRODUCCIÓN

Con el gran auge de los computadores personales a principios de los años ochenta, también se incrementaron los delitos penales como el fraude, el robo de dinero y el espionaje industrial y militar. Durante este período, se dieron a conocer nuevas modalidades de delitos, los informáticos, y por ende surgió la necesidad de identificarlos y tipificarlos.

La rama de investigación de delitos informáticos se desarrolló durante este período como un método para la recuperación e investigación de pruebas digitales con fines legales. Desde entonces, el alcance del delito ha aumentado rápidamente.

El fenómeno de la criminalidad informática es cada vez más intenso y variado; su presencia cambia constantemente, adaptándose a las nuevas posibilidades brindadas por la tecnología. De forma concreta, para hablar sobre delitos informáticos es importante mencionar las conductas de acceso no autorizado a sistemas informáticos, acciones destructivas en esos sistemas, la interceptación de comunicaciones, modificaciones de datos, infracciones a derechos de autor, incitación al odio, a la discriminación, el escarnio religioso, el tráfico de pornografía infantil, terrorismo, fraudes, entre otros.

Con tal aseveración, se observa que el ciberespacio es campo para la comisión de delitos que ya se tipifican en el ordenamiento jurídico, sin embargo, puede abarcar conductas aún no incriminadas, pero altamente dañinas. Esto debido a su vulnerabilidad intrínseca, que puede ser verificada por las siguientes características:

Capacidad de procesar, guardar y circular, de forma automatizada y, en tiempo real, grandes cantidades de información en formato digital de los más variados (fotos, películas, sonidos).

El número enorme de usuarios, la frecuencia con que acceden, la libertad que tienen para enviar, transferir, difundir y acceder a información, de modo que los internautas pasan a ser potenciales víctimas, pero potenciales sujetos activos de delitos;

Las características físicas, técnicas y lógicas de la tecnología de la información. Se logra acceso a archivos de las más distintas naturalezas ya los más variados programas informáticos.

La enorme potencialidad de multiplicación de las acciones ilícitas. La creación de foros de debates, páginas en Internet, comunidades de relaciones, pueden facilitar la práctica de delitos, pudiendo, además, dar mayor repercusión a ellos, como en las ofensas contra el honor, por citar un ejemplo.

De este modo el Derecho Penal se enfrenta a nuevas situaciones en cuanto a las prácticas delictivas, debiendo haber ponderaciones sobre nuevos modus operandi. Sumado a ello, hay que tener en cuenta los bienes jurídicos tutelados para que se defina con más claridad los delitos informáticos. Es lo que se verá al hablar sobre los bienes jurídicos.

A primera vista, uno puede preguntarse por qué es necesario definir un código de ética particular en el caso de delitos informáticos. No nos detenemos con las ofensas asociadas con el manejo de registros, el automóvil o la televisión. ¿Por qué el instrumento del delito haría la diferencia? No es un robo siempre un robo, ya sea cometido por un delito o usando una terminal de computador. Se puede responder que la ley no solo se ocupa de los fines ilícitos de un acto, sino también de los medios utilizados para lograrlos.

Con la aparición de las nuevas tecnologías, en especial la tecnología informática, no se crearon nuevos delitos, al igual que con la llegada de los automotores no se creó el robo, lo que si apareció fue la utilización de estas tecnologías para delinquir. El uso delictivo de computadoras ha aumentado la vulnerabilidad de la sociedad y en la medida en que la definición de los delitos y la adopción de medidas legislativas para prohibir ciertos actos tienen la intención de garantizar protección de la sociedad, la tecnología de la información es un área legítima de preocupación dentro del derecho penal.

Las leyes no solo deben permitir la reparación de los errores o el castigo de los delincuentes; también es esencial para ellos proscribir ciertos actos y la complejidad de los delitos informáticos justifica un trato especial.

2. DEFINICIÓN DE DELITO INFORMÁTICO

La informática se define como *"aquella ciencia que se dedica a estudiar el tratamiento de la información mediante medios automáticos, es decir, la ciencia de la información automática. Se trata de una sumatoria de conocimientos científicos y de técnicas que posibilitan el tratamiento automático de la información mediante el uso de computadoras".*

En opinión del autor de este ensayo, el delito informático es la conducta, típica, antijurídica y culpable llevada a cabo por medio de un sistema tecnológico informático, es decir cualquier acto ilegal, en el que el sistema informático, actúa como medio con el cual se comete el delito o como un instrumento utilizado para cometer actos delictivos.

A medida que los sistemas informáticos se generalizan cada vez más, y la comunidad empresarial confía cada vez más en los computadores y, a menudo, almacena información confidencial sobre ellas.

Así como el advenimiento de los vehículos automotores ha dictado cambios en las leyes penales, los equipos informáticos también están imponiendo cambios. La informática plantea preguntas aún más fundamentales. De hecho, debemos distinguir entre los diferentes tipos de delitos informáticos es decir, entre aquellos en los que el equipo informático es "el instrumento" de la ofensa y aquellos en los que es "el objeto" .

2.1. EL EQUIPO INFORMÁTICO COMO INSTRUMENTO DEL DELITO.

En este caso, el equipo informático es el medio para un fin. Por ejemplo, el delincuente puede modificar un programa contable para encubrir la malversación de fondos o el lavado de activos, puede realizar una alteración de los datos de los beneficiarios del Bono de Desarrollo Humano. En cada caso, el delincuente usa el computador como un instrumento de su ofensa. El medio es nuevo, pero la intención y el propósito del delito son siempre los mismos; apropiarse ilegalmente de la propiedad de otros.

2.2. EL EQUIPO INFORMÁTICO COMO OBJETO DEL DELITO.

Este tipo de delito no está limitado al robo de un computador como objeto físico tal, sino que abarca cualquier propiedad intangible almacenada en ella y cuyo valor es considerable. Por ejemplo, la información contenida en el

dispositivo de almacenamiento puede ser invaluable para su propietario y para terceros, y un delincuente puede apropiarse de ella sin causar un daño aparente en el computador o privar a su dueño de esta información. Este tipo de robo se aplica quizás a la información más valiosa del computador, el software.

3. DESARROLLO DEL TEMA.

Cuando el uso de Internet se volvió “comercial” , se volvió lo suficientemente accesible y fácil de acceder para la gente común, (aquellos que no eran docentes y personas vinculadas con el gobierno), era una nueva frontera, en su gran mayoría no estaba regulado; los legisladores no habían anticipado el rápido crecimiento o los tipos de comportamientos en línea que requerirían las nuevas leyes para proteger a los usuarios bien intencionados.

En más de dos décadas desde entonces, los gobiernos han aprobado muchos estatutos para abordar el problema de las actividades delictivas que tienen lugar a través de Internet. El acoso cibernético, robo de servicios inalámbricos, correo no deseado, acceso no autorizado, la mayoría de estas leyes no existían hace veinticinco años.

Entonces ahora tenemos muchas leyes en los libros, pero hacerlas cumplir es otro asunto. Puede ser frustrante para las víctimas de estos delitos, que los perpetradores nunca comparezcan ante la justicia. Algunos departamentos de policía locales han establecido divisiones específicamente dedicadas a la aplicación de crímenes informáticos, pero algunos evitan investigar y hacer cumplir este tipo de delitos. Eso se debe a que, por una serie de razones, hacer cumplir las leyes que rigen el comportamiento en línea es intrínsecamente más difícil que la aplicación de las leyes "tradicionales". En seguida se mencionarán algunos de esos motivos.

3.1. ANONIMATO E IDENTIDAD

Antes de que la jurisdicción entre en juego, es necesario descubrir dónde y quién es el delincuente antes de que se pueda pensar en realizar un arresto. Este es un problema con los delitos en línea, porque existen muchas maneras de ocultar la identidad. Existen numerosos servicios que enmascararán la dirección IP de un usuario distribuyendo el tráfico a través de varios servidores, esto hace que sea difícil rastrear al delincuente.

Algunos estudios han demostrado que es más probable que las personas participen en actividades ofensivas y / o ilegales en línea debido a la percepción de anonimato.

Sin embargo, los intentos por rastrear mejor la identidad en línea plantean serios problemas para los defensores de la privacidad y provocan reacciones

políticas negativas. Y el fin del anonimato en Internet podría tener graves consecuencias en los países donde el gobierno castiga a los disidentes, por lo que incluso si se superara el desafío tecnológico de identificar a cada usuario en línea, muchos legisladores vacilarían en exigirlo. Los delincuentes informáticos explotan los derechos y privilegios de una sociedad libre, incluido el anonimato, para beneficiarse a sí mismos.

Si bien el anonimato en línea aún se puede lograr, cada vez es más difícil. Con un trabajo diligente, a menudo es posible rastrear a los delincuentes por IP y por pistas que pueden dejar dentro del contenido de los datos. Muchos delincuentes informáticos no son especialmente conocedores de la tecnología, como los que usan Internet para cometer fraude o ciberacoso. Muchos de los que están más informados sobre la tecnología todavía dejan pistas porque se vuelven descuidados o son arrogantes y excesivamente seguros.

3.2. NATURALEZA DE LA EVIDENCIA

Sin embargo, otra cosa que hace que el delito informático sea más difícil de investigar y enjuiciar en comparación con la mayoría de los demás delitos, es la naturaleza de la evidencia. El problema con la evidencia digital es que, después de todo, en realidad es solo una colección de unos y ceros representados por magnetización, pulsos de luz, señales de radio u otros medios. Este tipo de información es frágil y se puede perder o alterar fácilmente.

Proteger la integridad de la evidencia y mantener una cadena de custodia clara siempre es importante en un caso delictivo, pero la naturaleza de la evidencia en un caso de de delito informático, hace que ese trabajo sea mucho más difícil. Un investigador puede contaminar la evidencia simplemente examinándola, y los delincuentes informáticos sofisticados pueden configurar sus computadoras para destruir automáticamente la evidencia cuando acceda cualquier persona que no sea ellos mismos.

En casos como la pornografía infantil, puede ser difícil determinar o probar que una persona descargó el material ilegal a sabiendas, ya que otra persona puede piratear un sistema y almacenar datos en su disco sin el conocimiento o permiso del usuario, esto si el sistema no es adecuadamente seguro.

En casos de intrusión no autorizada, el delincuente a menudo borra todos los registros que muestran lo que sucedió, de modo que no hay evidencia que demuestre que un crimen haya ocurrido, y mucho menos de dónde vino el ataque.

3.3. LA INFORMÁTICA FORENSE.

La definición forense de la computadora se puede dividir en varios aspectos técnicos de la ciencia real de la informática forense. La definición general de informática forense es el proceso y los métodos de investigación utilizados para encontrar evidencia digital y prepararla para procedimientos legales. La definición más profunda incluye la preservación de los medios y los datos, la identificación de la evidencia relacionada con la computadora, la extracción de los datos y la interpretación. La interpretación es quizás el elemento más importante de la definición forense de la informática porque es aquí donde los expertos forenses deben sacar conclusiones de un análisis forense formal.

Informática forense implica la aplicación de técnicas de investigación y análisis informático para resolver un delito y proporcionar pruebas para respaldar un caso. Los investigadores a menudo usan aplicaciones forenses patentadas y programas de software para examinar los discos duros de los computadores, extraer ciertos tipos de datos de archivos y carpetas, y también para recuperar información de archivos encriptados. Esta información digital debe estar organizada y documentada en un formulario de informe oficial para ser presentado en un tribunal de justicia.

A lo largo del proceso de recopilación e interpretación de datos, el especialista en informática forense debe documentar todo de forma estructurada. Deben informar exactamente qué tipos de investigaciones se realizaron y documentar todos los pasos tomados para recuperar varios archivos, carpetas y datos. Las partes procesales pueden aplicar varios tipos de metodologías y testimonios para determinar si la evidencia presentada puede ser utilizada en los procedimientos legales. Esta es la razón por la cual los especialistas en informática forense deben conocer los diferentes procesos legales involucrados en una investigación y asegurarse de que siempre haya un alto nivel de integridad de la evidencia.

Es importante reconocer que existen dos tipos principales de investigaciones forenses informáticas, por lo que la definición forense informática puede cambiar. El primero involucra investigaciones en las que se utilizó un computador o tecnologías digitales para realizar el delito. El segundo es cuando un computador se utiliza como objetivo de un delito.

La informática forense ha recorrido un largo camino, y hay herramientas disponibles para los investigadores que les permiten examinar evidencia digital sin alterarla. Los examinadores forenses capacitados pueden conservar de manera confiable los datos para su presentación ante un tribunal e incluso recuperar los datos eliminados, y el sistema legal está evolucionando y se están adoptando nuevos procedimientos para abordar los desafíos especiales presentados por la naturaleza de la evidencia digital.

Los problemas jurisdiccionales aún presentan un desafío, particularmente cuando el delincuente se encuentra en otro país, pero cada vez más entidades gubernamentales están reconociendo el daño que el delito cibernético les hace a sus ciudadanos y están trabajando juntos. Los países están cooperando para adoptar leyes consistentes y formar equipos de trabajo interjurisdiccionales para tratar el delito informáticos que cruza las fronteras internacionales.

3.4. EL CONVENIO DE BUDAPEST SOBRE LA CIBERDELINCUENCIA.

Firmado el 23 de noviembre del 2001, por ahora es el único convenio internacional importante en la lucha contra los delitos informáticos, esta convención trata las posibles infracciones como son las de derechos de autor, seguridad de la red informática, fraude en general y la lucha contra la pornografía infantil. A este convenio se han unido 66 países de todo el mundo. Hasta el momento, por América latina solo lo han hecho Argentina, Chile, Colombia, Costa Rica y República Dominicana.

En vista del crecimiento de este tipo de delincuencia y del desarrollo cada vez mayor de las tecnologías, este convenio debe evolucionar constantemente junto con las prácticas de las autoridades.

Asimismo, cada 18 meses, se celebra una gran reunión internacional con todos los actores interesados. Estas conferencias permiten hacer un inventario de las nuevas prácticas problemáticas que aparecen.

3.5. LOS DELITOS INFORMÁTICOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP).

Pese a que varios artículos del COIP contienen el vocablo "informático" o "informática", no todos estos artículos se relacionan con el concepto de delito informático antes indicado en este ensayo.

Después de realizar una indagación de los artículos que conforman el COIP, se describen a continuación aquellos que tienen directa relación con los delitos informáticos propiamente dichos:

- **Art. 190**.- Apropiación fraudulenta por medios electrónicos.
- **Art. 211**.- Supresión, alteración o suposición de la identidad y estado civil.
- **Art. 229**.- Revelación ilegal de base de datos.
- **Art. 231**.- Transferencia electrónica de activo patrimonial.
- **Art. 232**.- Ataque a la integridad de sistemas informáticos.
- **Art. 234**.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

Existen artículos en el COIP que, si bien es cierto, contemplan el uso de tecnologías informáticas, no deberían ser considerados como delitos informáticos. Estos son los siguientes:

- ***"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; será sancionada con pena privativa de libertad de trece a dieciséis años…"*

La finalidad del artículo 103 del COIP es la de sancionar la producción y difusión de pornografía infantil, mas no el uso doloso de la tecnología informática; el artículo menciona los diferentes medios que pueden ser utilizados con este propósito; sin embargo, en el medio informático es uno de los muchos medios mencionados.

- ***"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."*

  Este artículo tiene como fin la protección de la intimidad de las personas, indica que la violación a ésta, será sancionada, fuere por cualquier medio, no hace referencia al medio informático de manera exclusiva.

Adicionalmente, el COIP cuenta con un artículo muy interesante, en el cual, dependiendo del modo en el que se lleve a cabo el delito, podría constituirse o no, en un delito informático. El artículo es el siguiente:

***"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."*

Hasta aquí, este artículo no contempla, necesariamente, un delito informático, ya que no especifica la causa de la destrucción o inutilización de la información clasificada. Éste lo sería si la forma para inutilizar la información fuese un medio tecnológico informático.

Analizando el párrafo siguiente del artículo 233, el cual dice que: *"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…"; se concluye que en efecto se trata de un delito informático, ya que en se menciona claramente la utilización de "*cualquier medio electrónico o informático*" para cometer el delito.

4. LOS BIENES JURÍDICOS Y SU AFECTACIÓN POR LOS DELITOS INFORMÁTICOS

La mayor parte de la doctrina entiende que la función del derecho penal es la protección de los bienes jurídicos, de modo que es imprescindible conocer el interés jurídicamente protegido para que se obtenga la más adecuada interpretación de la norma. Se tiene, además, como cierto, que es el legislador el responsable de la elección de los bienes que deben recibir la protección estatal.

El concepto de bien jurídico sólo aparece en la historia dogmática a principios del siglo XVIII.. Antes de eso, época en que el exponente principal fue Beccaria, el derecho penal vivió una situación bastante autoritaria donde las conductas delictivas eran definidas indeterminadamente. No se hizo distinción de los mandamientos de Dios del estatuto de los hombres, siendo el delito, sobre todo un pecado. Hoy las ideas son otras, pero hay varias acepciones para el término. Es innegable, sin embargo, que la doctrina mayoritaria entiende ser una limitación del poder punitivo del Estado. Y eso es fundamental en la verificación si estamos en un Estado Democrático de Derecho o en Estado autoritario.

Hubo y todavía hay discusiones en el sentido de evolución en el concepto de bien jurídico. Para su estudio, debemos trazar un marco divisorio entre las teorías clásicas y las modernas y, también, entre bienes individuales y colectivos.

Bajo la perspectiva individual, los bienes jurídicos son aquellos valores que deben recibir mayor protección estatal.

Ante las nuevas tendencias sociales, ocurre el fenómeno de la "desmaterialización" de los bienes jurídicos. Así, no sólo el Derecho Penal castiga ataques directos a los bienes jurídicos, como también incrimina conductas que frecuentemente no pasan de mera transgresión a una norma organizativa sin resultado concreto. Y eso se hace también por la creación artificial de bienes, de modo que se protegen intereses de acuerdo con fines institucionales, no necesariamente por tener sustento cultural o social.

Hay más que una tendencia, pero verdadero distanciamiento del típico entendimiento de bien jurídico, de visión antropocéntrica y orientado a bienes

particulares, hacia la tendencia de "desmaterialización" del bien jurídico, lo que, obviamente, influye en la teoría del delito.

Y aquí hay que comentar sobre bienes jurídicos informáticos. No hay como dejar de cuestionar nuevos intereses a ser protegidos por el Derecho Penal. Se observa claramente que, con respecto a medios tecnológicos, las ofensas pueden dirigirse no sólo a los valores ya conocidos por nosotros y tradicionalmente vistos como relevantes (vida, fe-pública, patrimonio), sino también la información almacenada en diversos dispositivos, la seguridad de los sistemas y de las redes informáticas y de telecomunicaciones.

La confiabilidad en los sistemas y en los datos debe ser visto como nuevo interés a ser protegido.

Según Romeo Casabona y Bueno Arus eso no significa que los bienes tradicionales sean dejados de lado, ya que puede haber violación conjunta de bienes tradicionales y de otros, más recientes. Así, un ataque a un sistema informático puede violar el patrimonio (si ha habido, por ejemplo, transferencia de valores sin autorización), pero también la seguridad de las redes. Bajo esta óptica, los delitos informáticos pueden ser vistos como pluri ofensivos (violan bienes jurídicos tradicionales y otros, peculiares a la sociedad de la información).

En ese sentido, se tiene que el concepto de bien jurídico es un objeto cuya importancia para el ser humano se demuestra tan válida que es necesario tutelarlo jurídicamente a fin de protegerlo.

La idea traída por el bien jurídico, objeto a ser tutelado por el Derecho Penal, es que es tan importante en el ámbito social, que el Derecho debe ser responsable de cuidarlo para que no sea transgredido; y el rama responsable de la protección es la rama penal, de modo que es necesario un cierto cuidado con lo que es resguardado: no todo objeto importante para el ser humano debe ser cubierto por el Derecho Penal. Así, se tiene que la noción de bien *stricto sensu* está presente en el concepto de bien jurídico pero no debe confundir, de modo que no todo bien se considerará bien jurídico.

Además, la noción de bien jurídico está ligada a la coyuntura en que se encuentra determinada sociedad, ya que cada una de ellas presenta demandas distintas, resultando en una tutela diferenciada. Así, los valores sociales se modifican a medida en que pasan las generaciones, que traen

consigo nuevos pensamientos e ideales, para alterar sustancialmente lo que se considera esencial y pasible de tutela por el Derecho Penal

Las sociedades primitivas, por ejemplo, se construían en torno a ideales sagrados, y por eso es fácil entender por qué los crímenes eran conductas tenidas como actos contrarios a lo divino. Con el advenimiento del iluminismo y de las teorías racionalistas, el delito pasó a ser identificado como la violación del contrato social o de un derecho subjetivo.

Según Roxin, en la actualidad, el legislador ganó un papel importante en la identificación del objeto a ser tutelado por el Derecho Penal. Esto porque se cuestiona mucho si la tarea del derecho penal se determina por la protección de bienes jurídicos

Como una concepción dogmática del bien jurídico, el legislador no lo crea por medio la norma, sólo constata su existencia en el mundo jurídico y su importancia en la sociedad.

Una vez que el objetivo principal es analizar el bien jurídico como una consagración constitucional y social y su incidencia en los delitos informáticos con el propósito de dedicar la importancia de un estudio apropiado de éste, y en el caso de que se trate de un delito. Por medio de una interpretación del Código Orgánico Integral Penal es posible identificar como bien jurídico de estos delitos, la inviolabilidad de los datos. Es importante señalar que tal protección también encuentra basadas demandas sociales, ya que Internet es uno de los medios de comunicación más utilizados en el mundo y se ha convertido en una de las materias más relevantes.

5. CONCLUSIÓN

Se observa la constante ascensión de cuestiones informáticas frente al derecho de forma general como consecuencia de su desarrollo tecnológico e inclusión en los medios y actividades sociales. En especial, se percibe tal fenómeno en la rama penal, sea por la potencialización de conductas tipificadas, así como la demanda por tutela de conductas inexistentes, por ser sustancialmente vinculadas a las innovaciones informáticas. Tal ascenso, debido al alto grado de informatización social es acompañado por demandas populares que presionan a legisladores a crear políticas de forma rápida, pero ineficientes bajo un prisma dogmático, en ejercer su función esencial de proteger cierto bien jurídico.

El surgimiento de la tecnología y su desarrollo promueven constante revolución en nuestras vidas a pesar de que tal constatación no pueda ser eficazmente medida. No hay como negar, sin embargo, que la informática hace la vida más dinámica, más práctica, facilitando sobre todo la vida social. Por otro lado no se puede creer ciegamente que tal tecnología sea perfecta, porque, después de todo, quien la produce es el ser humano, falible y ciertamente susceptible a errores.

Hay gran preocupación por el desarrollo de la tecnología, pero se dejan de lado cuestiones importantes como regulaciones en cuanto al trato de la misma o, aún, sobre métodos y leyes que busquen frenar la nueva ola delictiva.

De esta forma, entre las varias cuestiones que circundan la delincuencia informática, hay que analizar el actual estado de las legislaciones penales, no sólo la Ecuatoriana, sino también las extranjeras, ya que para la total protección penal en cuanto a esos ilícitos es necesaria alguna armonización internacional.

También sería recomendable modificar las perspectivas y enfoques penales, especialmente para evitar la pérdida de relevancia y significado social de tal rama jurídica. Por eso es relevante entender los delitos informáticos como verdaderas conductas de riesgo, promoviendo algunas incriminaciones valiéndose de tipos de peligro. Así, por ejemplo, un mero acceso no autorizado al sistema debe interpretarse como una verdadera pérdida de credibilidad y confianza en el funcionamiento del sistema.

6. RECOMENDACIÓN

Considerando la relevancia del tema, serian necesario una mayor cautela y consideración de los legisladores. Muchas veces la tipificación ocurre sin el debido estudio del tema y de los bienes que, definitivamente deben ser protegidos, de modo que resulte en la no criminalización de conductas que deberían ser criminalizadas, o en un tratamiento que no lleva a la protección efectiva y eficaz de tales delitos. Por lo tanto, se defiende que antes de la criminalización de las conductas que mantiene relación con la informática se debe hacer un estudio acerca del bien jurídico, con respaldo de la Constitución y en lo que es reclamado por la sociedad, como de la parte técnica de la reforma, a fin de que la ley o el tipo penal se hagan de manera más precisa y clara, facilitando su aplicación y el alcance de su fin.

BIBLIOGRAFIA:

Concepto de informática http://concepto.de/informatica/#ixzz59VOcC1lJ

Romeo Casabona, C. (1988.) *La protección penal del software en el* derecho español. Actualidad Penal. Granada: Comares.

Romeo Casabona, C. (2006.) *De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal.* Granada: Comares.

Ministerio De Justicia, Derechos Humanos Y Cultos (2014). Código Orgánico Integral Penal. –Quito: Gráficas Ayerve C. A.

VLADIMIR ARAS. Crimes de Informática. (2001). Recuperado de: Https://jus.com.br/artigos/2250/crimes-de-informatica/

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Jorge Adrián Hidalgo Pazmiño**, con C.C: # 1714097761, autora del trabajo de titulación: **Los delitos informáticos y su afectación sobre los bienes jurídicos** previo a la obtención del título de **Abogada de los Tribunales y Juzgados de la República** 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 de 2018

f. _____

Jorge Adrián Hidalgo Pazmiño

C.C: **1714097761**

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	Los delitos informáticos y su afectación sobre los bienes jurídicos		
AUTOR(RES):	Jorge Adrián Hidalgo Pazmiño		
REVISOR(ES)/TUTOR(ES):	Ab. Edgar Escobar Zambrano, Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia y Ciencias Sociales y Políticas		
CARRERA:	Carrera De Derecho		
TITULO OBTENIDO:	Abogada de los Tribunales y Juzgados de la República		
FECHA DE PUBLICACIÓN:	20 de febrero de 2018	**No. DE PÁGINAS:**	27
ÁREAS TEMÁTICAS:	Derecho, Derecho penal, Derechos humanos		
PALABRAS CLAVES/ KEYWORDS:	Delitos informáticos, bienes jurídicos		

RESUMEN/ABSTRACT (150-250 palabras):
En los últimos años, Internet ha crecido explosivamente. En comparación con los 26 millones de usuarios enumerados en 1995, hoy en día más de 200 millones de personas se comunican, compran, pagan facturas, comercian e incluso consultan a su médico en Internet. Mientras Internet estaba en auge, el crimen en línea también estaba creciendo. Los delincuentes informáticos, como se los llama, han invadido o invadido en gran medida el mundo virtual, cometiendo delitos tales como el uso de códigos de acceso confidenciales, piratería informática, fraude, sabotaje informático, tráfico de drogas, pornografía pedófila y "acoso cibernético". Los delincuentes informáticos son tan variados como las diferentes formas de delincuencia que practican. Pueden ser estudiantes, terroristas o criminales organizado. Los delincuentes informáticos pueden cruzar las fronteras a un ritmo rápido, pasar desapercibidos, ocultos detrás de innumerables "enlaces" o simplemente desaparecer sin dejar rastro. Pueden pasar las comunicaciones a través de "paraísos de datos" u ocultar la evidencia de sus delitos.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	Teléfono: +593-9-99071727	E-mail: Jahp_77@hotmail.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):	