UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

TÍTULO:

"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"

TESIS PREVIO A LA OBTENCIÓN DEL TITULO DE ABOGADA

AUTORA:

Carolin Anabel Ruiz Cruz

DIRECTOR:

Dr. Marcelo Armando Costa Cevallos Mgs. Sc.

Loja – Ecuador

2016

CERTIFICACIÓN

DR. MARCELO COSTA CEVALLOS MG. SC.
DIRECTOR DE TESIS

CERTIFICO:

Haber revisado el trabajo de investigación de tesis intitulado "ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS" presentado por la postulante CAROLIN ANABEL RUIZ CRUZ, mismo que cumple con todos los requisitos de fondo y forma, ajustándose de esta manera a las normas estatutarias y reglamentarias de la Universidad Nacional de Loja.

Por lo tanto, autorizo su presentación, disertación y defensa.

Loja, Diciembre del 2016

DR. MARCELO COSTA CEVALLOS MG. SC.
DIRECTOR DE TESIS

AUTORÍA

Yo, CAROLIN ANABEL RUIZ CRUZ, declaro ser la autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

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

Autora: Carolin Anabel Ruiz Cruz.

Firma 

Cédula: 1104775067

Fecha: Loja, Diciembre del 2016.

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DE LA AUTORA, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, **CAROLIN ANABEL RUIZ CRUZ,** declaro ser la autora de la tesis titulada: **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS",** como requisito para optar el grado de **ABOGADA**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional;

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 01 días del mes de Diciembre del dos mil dieciséis, firma la autora.

Firma: .....

Autora: Carolin Anabel Ruiz Cruz.

Cédula: 1104775067

Dirección: Loja.Barrio El Rosal Dirección. Carlos Mariategui y Ciro Alegría

Correo electrónico: carito.xoxo@hotmail.com

Teléfonos: 072710429 **Celular:** 0989560259

Datos complementarios:

Director de Tesis: Dr. Marcelo Costa Cevallos Mgs. Sc

Tribunal de Grado:

Dr. Augusto Astudillo Ontaneda	**Presidente**
Dr. Darwin Quiroz Castro Mg	**Vocal**
Dr. Carlos Manuel Rodríguez	**Vocal**

AGRADECIMIENTO

Mi inmensa gratitud a la Universidad Nacional de Loja, por permitirme acceder a mis estudios de nivel superior.

A las autoridades de la Modalidad de Estudios a Distancia, y de manera especial a la Dr. Marcelo Costa Mgs., por haber asumido con absoluta responsabilidad y dedicación, la dirección de este trabajo, y colaborar con su orientación para que el estudio se realizara en la mejor forma posible.

La Autora.

DEDICATORIA

Dedico mi esfuerzo y tenacidad a mis seres amados, mi esposo e hija, que son el motivo de superación para ser cada día mejor, y como soporte en mi futura carrera profesional.

CAROLIN ANABEL

1. TÍTULO.

“ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS”

2. RESUMEN.

La presente investigación denominada ““ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS” tiene como objeto dar una visión clara sobre los delitos informáticos en especial sobre la violación de los derechos constitucionales de los ciudadanos, que se generan por la utilización de las tecnologías de la información y de la comunicación, como el correo electrónico, transacciones financieras, comercio electrónico y la utilización de las redes sociales; se analiza y conceptualiza la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales y se establecen alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

Para desarrollar la presente investigación, se utilizaron métodos, procedimientos y técnicas de investigación científica, que permitirán el desarrollo de la investigación, como lo Bibliográfico – Documental, Linkográfía, e investigación de campo.

Las técnicas utilizadas fueron la entrevista, que se aplicó a 30 profesionales de la abogacía en libre ejercicio y que tienen relación con la temática a investigar; la encuesta efectuada a 30 ciudadanos comunes, en la que permitió levantar información con respecto a su percepción de los delitos informáticos y sobre la vulnerabilidad de sus derechos constitucionales.

Dentro de las principales conclusiones, se puede manifestar que existe la necesidad legal en cuanto a la tipificación del delito informático, como la apropiación de la información y la intimidad personal en las redes sociales, y debe considerárselo acto antijurídico y ser causa de sanción y considerárselo como delitos informáticos, ya que afectan la privacidad de una persona, y al colectivo en general.

En necesario incluirse en la legislación penal ecuatoriana, la tipificación del delito informático, como la apropiación de la información y la intimidad personal en las redes sociales y debe considerárselo acto antijurídico y ser causa de sanción, y reformar la legislación constantemente, ya que las tecnologías de la información y la comunicación están en desarrollo constante.

2.1. ABSTRACT.

This research called "" ANALYSIS OF COMPUTER CRIMES AND VIOLATION OF THE CONSTITUTIONAL RIGHTS OF CITIZENS "aims to give a clear picture on cybercrime in particular on the violation of constitutional rights of citizens, which are generated by the use of information technology and communication, like e-mail, financial transactions, electronic commerce and the use of social networks; It analyzes and conceptualizes the nature of computer-related offenses and their characterizations according to their main characteristics and alternative solutions are set to punish computer crimes and prevent the violation of the constitutional rights of the victim.

Documentary, Linkography, and field research - to develop this research, methods, procedures and techniques of scientific investigation that will enable the development of research, as bibliographic were used.

The techniques used were the interview, which was applied to 30 legal professionals in free practice and having regard to the issues to investigate; The survey of 30 ordinary citizens, which allowed to gather information regarding their perception of cybercrime and the vulnerability of their constitutional rights.

Among the key findings, it can say that there is a legal requirement in respect to the definition of computer crime, such as the appropriation of information and personal privacy in social networks, and should consider offense and sanction

cause and consider as computer crime, affecting the privacy of a person, and the group in general.

It is necessary to include in Ecuador's criminal law, the definition of computer crime, such as the appropriation of information and personal privacy in social networks and must consider unlawful act and cause penalty and amend legislation constantly, since technologies Information and communication are constantly evolving.

3. INTRODUCCIÓN.

El derecho y la tecnología en los últimos años contribuyó a que la sociedad de un giro total en el desarrollo de su vida, hoy el uso de la tecnología, se hace indispensable para la sociedad, y esto ha dado como resultado que en el campo del derecho se agregue una nueva ciencia jurídica como es el derecho informático.

Los delitos informáticos, los fraudes informáticos, implican actividades como fraudes, falsificaciones, perjuicios, estafa, sabotaje, haciendo uso indebido de las computadoras; por ello es necesario propiciar su regulación y control en la legislación ecuatoriana.

Una de las razones para que los delitos informáticos, vaya en aumento, se debe principalmente a la dificultad de identificar y descubrir a los autores intelectuales, quedando muchos de estos delitos en la impunidad, generando progresivamente que la sociedad pierda la confianza en una justicia eficaz, eficiente y oportuna; de acuerdo a lo manifestado, es necesario que el estado ecuatoriano, proteja a los mandantes, reformando la legislación ecuatoriana, para identificar la manera adecuada de hacer publicidad política y de esta forma construir una nueva manera del quehacer político en el Ecuador.

Con estos antecedentes, el problema de investigación del presente trabajo, se relaciona con los delitos informáticos, violentan y lesionan los derechos

constitucionales de los ciudadanos, y en muchos casos, los delitos quedan en la impunidad, por la dificultad de descubrir a los autores.

La presente investigación, está estructurado inicialmente con una parte preliminar, en la que se incluye el resumen en español e inglés, de la misma forma que una introducción; Dentro de la revisión de literatura, se abordan el marco conceptual, marco doctrinario y marco jurídico; a continuación se describe la metodología en la que constan los métodos y técnicas, procedimientos utilizados. La parte esencial de la investigación, lo comprende los resultados, en la que se describen en forma tabular y gráfica los datos obtenidos, a los cuales se deriva un análisis e interpretación; de la misma forma la discusión en la que se realiza la verificación de objetivos planteados. Finalmente se redactan las conclusiones, recomendaciones.

4. REVISIÓN DE LITERATURA.

4.1. MARCO CONCEPTUAL.

EL DELITO.

"El delito es el hecho humano previsto de modo típico por una norma jurídica sancionada con pena en sentido estricto, lesivo o peligroso para los bienes o intereses considerados merecedores de la más; enérgica tutela y expresión reprobable de la personalidad del agente, tal cual es el momento de su comisión".

La noción sustancial del delito enumera los elementos constitutivos del delito, que son:

- El delito es un acto humano (acción ú omisión); se origina pues en la actividad humana, quedan descartados los hechos que son anormales, los acontecimientos fortuitos.
- El delito es un acto humano antijurídico, está en oposición a la norma jurídica, debe lesionar o poner en peligro un bien jurídicamente protegido.
- Debe ser al mismo tiempo conducta típica o sea que corresponde a un tipo legal, definido por ley. Debe ser culpable, es decir, imputable a dolo o culpa y que puede ligarse a una persona.

- Debe ser sancionable con una pena, pues sin ella la acción o la omisión no existen.[1]

CLASIFICACIÓN DE LOS DELITOS.

Cada año, el FBI hace una recopilación uniforme de datos sobre el crimen en los Estados Unidos y publica estadísticas de los distintos delitos como parte del programa llamado Uniform Crime Reporting (UCR). Los informes no solo brindan estadísticas útiles, sino también clasificaciones y definiciones de los delitos. El programa UCR categoriza los delitos graves como “Delitos de la Parte Uno” y los delitos menos graves como “Delitos de la Parte Dos”.

DELITOS DE LA PARTE UNO.

Delitos de violencia contra las personas.

Agresión agravada: ataque ilegal a otra persona para causarle lesiones corporales severas o muy graves. Generalmente, este tipo de ataque es acompañado con un arma o cualquier otro medio con probabilidad de producir la muerte o un daño físico grave. El intento de agresión agravada, que implica el uso o la amenaza de usar un arma de fuego, un cuchillo o cualquier otro tipo de arma, se incluye dentro de esta categoría de delito, ya que es probable que la persona atacada resulte gravemente lesionada.

---

[1] *RANIERI, Silvio Derecho Penal: Teoría del Delito, México, 1997.*

Asesinato: acción de matar a una persona intencionalmente.

Robo (robbery, en inglés): acción de quitar o intentar quitar algo de valor a una persona por la fuerza o amenazándola con usar fuerza o violencia. En este tipo de robo, una víctima está presente mientras ocurre el crimen.

Violación con uso de violencia: el "acceso carnal con una mujer por la fuerza y contra su voluntad". El UCR incluye las agresiones y los intentos de cometer violación por la fuerza o la amenaza de usar la fuerza, pero excluye la violación de menores (sin empleo de la fuerza) y otros tipos de delitos sexuales. El UCR recolecta únicamente información sobre violación de mujeres.

Delitos contra la propiedad.

Hurto (larceny-theft, en inglés): acción de tomar ilegalmente algo ajeno (p. ej. apropiarse de una bicicleta o tomar partes de automóviles, llevarse mercancía de una tienda sin pagarla o agarrar carteras de bolsillo) sin empleo de la fuerza, violencia o sin cometer fraude. También se incluye el intento de hurto.

Hurto de vehículos motorizados: el hurto o el intento de hurto de un vehículo.

Incendio intencional: acción de quemar o intentar quemar una casa, edificio público, vehículo motorizado, aeronave o propiedad personal, deliberada o maliciosamente, con o sin la intención de estafar.

Violación de domicilio: acción de entrar ilegalmente a una propiedad para cometer un delito o hurto. No implica necesariamente ingresar por la fuerza.

DELITOS DE LA PARTE DOS.

Adulteración de documentos: la adulteración de documentos implica crear o alterar un documento escrito de manera tal que los derechos de otra persona quedan comprometidos. La falsificación consiste en realizar copia o imitación de un objeto sin autorización y hacer pasar dicha copia como si fuera el objeto genuino u original. Aunque en la mayoría de los casos la falsificación está relacionada con el dinero, también puede aplicarse a las prendas de vestir y los accesorios fabricados para aparentar que son productos de diseño original.

Armas (portación ilegal, etc.): el hecho de portar un arma oculta sin la licencia o el permiso correspondiente; obtener un arma, una licencia o municiones de manera fraudulenta; o poseer un tipo de pistola o arma de asalto cuya propiedad, portación o cuyo uso no esté autorizado al público.

Conducir en estado de ebriedad o intoxicación: acción de manejar un vehículo bajo los efectos de alcohol o drogas. Cada estado establece el nivel de alcohol en sangre permitido para los conductores.

Conducta contraria al orden público: comportamiento que constituye una amenaza potencial para uno mismo o para otras personas. A veces, las leyes que regulan este tipo de conducta se superponen con las leyes de ebriedad en público.

Delito contra la familia (incumplimiento de la obligación de manutención, etc.): el que comete uno de los padres, o ambos, al no sustentar a sus hijos.

Delito sexual (violación de menores, etc.): el que comete un adulto al mantener relaciones sexuales con un niño o adolescente que no tiene capacidad legal para dar su consentimiento.

Desfalco: apropiación indebida de dinero o bienes que una persona tiene a su cargo para uso y beneficio personal.

Ebriedad en público: estar ebrio en público durante un tiempo prolongado. Cada estado establece los niveles de alcohol en sangre que regulan este tipo de violación. Las leyes también disponen cuándo y dónde las personas tienen permitido llevar bebidas alcohólicas en envases abiertos.

Fraude: acto de engañar intencionalmente a una persona para obtener maliciosamente la posesión o el control de su dinero, bienes o derechos específicos.

Fuga: en general, los estados clasifican el acto de huir del hogar como un delito que resulta de un estado o condición, especialmente cometido sólo por menores de edad. El objetivo del programa Amber Alert del Departamento de Justicia es ayudar a las comunidades a comenzar la búsqueda de niños ante la sospecha de que se encuentran en peligro y que no han dejado su hogar de manera voluntaria.

Juegos por dinero ilegales: aquellos prohibidos por la ley, ya sea local, estatal o federal. Aunque en muchos estados los juegos por dinero están permitidos, las

personas deben asegurarse de participar sólo en aquellos tipos de juegos que sean legales en los condados específicos donde éstos se permiten. La participación en estos juegos ilegales por Internet crea un obstáculo para los funcionarios encargados de aplicar la ley.

Propiedad robada (tráfico de): el hecho de vender o comprar bienes que han sido robados a otra persona o entidad.

Prostitución y delitos relacionados: el ofrecimiento de favores sexuales a cambio de dinero, drogas u otros bienes, o el hecho de brindar dichos favores.

Intento de agresión no agravada: el intento de ocasionar daño físico a otra persona estando ésta consciente del hecho. La agresión constituye un acto ilícito, el cual puede ser civil o penal, y la sanción correspondiente puede ser un castigo penal, o bien una indemnización por daños. “Violencia física contra una persona”, en general, se define como el hecho de tener un contacto físico con ésta ilícitamente. Sin embargo, en muchas jurisdicciones, no se tiene en cuenta esta distinción.

Vagabundeo: situación de quien no mantiene una dirección postal verificable y que pasa gran parte del tiempo deambulando en público.

Vandalismo: el acto de dañar o alterar la propiedad pública o privada sin permiso.

Violación de las leyes relacionadas con la venta de alcohol: la venta de bebidas alcohólicas sin licencia válida o la falta de control de la identificación de toda persona que desea comprar alcohol en un establecimiento.

Violación de leyes sobre drogas: violación de cualquier ley sobre drogas, ya sea local, estatal o federal, que prohíba la tenencia o venta de drogas específicas o de objetos relacionados con el consumo de drogas.

Violación del toque de queda/vagancia: a veces, la violación del toque de queda se clasifica como un delito que resulta de un estado o condición (un delito cometido sólo por menores de edad). La vagancia implica quedarse en un lugar determinado por un tiempo excesivo, sin poder justificar la presencia de uno en dicho lugar al ser interrogado por las autoridades. En general, la vagancia se comete junto con la violación del toque de queda.

DELITOS NUEVOS O DESTACADOS.

Crimen organizado: actualmente el crimen organizado, en general, implica la participación de pandillas callejeras locales; sin embargo los carteles internacionales de narcotráfico continúan ejercitando el contrabando de gran cantidad de drogas a los Estados Unidos. Muchos de estos grupos también son responsables de transportar por contrabando a los inmigrantes ilegales a este país.

Crimen de finanzas: según una teoría legal llamada “Doctrina de identificación”, las empresas pueden ser condenadas como entidades legales en conformidad con varias leyes penales. En un intento de combatir más a fondo este tipo de fraude, el presidente Bush firmó la Ley Sarbanes-Oxley de 2002 (Sarbanes-Oxley Act). Esta ley establece sanciones para aquellos que intenten cometer fraude contable.

Crimen motivado por prejuicios: aquellos delitos cometidos contra una persona debido a su raza, religión, origen étnico, orientación sexual u otras características personales. Las estadísticas del crimen motivado por prejuicios se encuentran en el reporte anual del FBI.

Robo de identidad: el uso ilegal de información personal de otra persona (p. ej. el número del seguro social, información de la licencia de conducir, el número de tarjeta de crédito) para obtener ganancias económicas. En mayo de 2006, el presidente Bush convirtió el Decreto 13,402 en ley, que autoriza el uso de recursos federales para combatir este delito, cuya incidencia es cada vez mayor.

Terrorismo: el uso o amenaza de usar violencia contra la población civil para cumplir objetivos políticos o ideológicos.[2]

ELEMENTOS DEL DELITO.

"Los elementos del delito son: la **Acción, la Tipicidad, la Antijuridicidad, la Imputabilidad y la Culpabilidad.** Son los componentes y características, NO independientes, que constituyen el concepto del delito.

[2] *http://espanol.getlegal.com/legal-info-center/clasificaciones-y-definiciones-de-los-delitos/*

LA ACCIÓN:

En la concepción causal la acción es la conducta humana dominada por la voluntad que produce en el mundo exterior un cambio determinado. Para la concepción finalista, la acción es conducta humana dirigida por la voluntad hacia un determinado resultado. Para la concepción social la acción es la realización voluntaria de consecuencias relevantes para el mundo social y voluntariamente realizadas por un ser humano.

LA ACCIÓN PENAL:

La Acción. Conducta voluntaria, que consiste en un movimiento de su organismo destinado a producir cierto cambio, o la posibilidad, en el exterior del mundo vulnerando una norma prohibitiva (Teoría de la causalidad).

La conducta activa debe exteriorizarse en el mundo material, si ocurre en el fuero interno y no llega a manifestarse, la acción, también, se excluye del campo delictivo

La posibilidad de cambio se da en los Delitos Frustrados y en la Tentativa. En estos delitos no es imprescindible que se produzca el cambio, en tal virtud quedan sujetos a sanción delictiva.

Debe ser realizada por el ser humano, con lo que se excluye a los animales y los fenómenos naturales.

La conducta debe estar dominada por la voluntad. Lo que excluye la conducta mecánica como ocurre en los supuestos de fuerza irresistible (condición de fuerza proveniente del exterior que actúa materialmente sobre el agente), acto reflejo (reacción automática y simple a un estímulo) o actos realizados en plena inconciencia (sueño, sonambulismo, hipnotismo). En estos supuestos no existe conducta, por tanto no hay delito.

SUJETOS DE LA ACCIÓN:

El sujeto de la acción es el ser humano.

No existe otros ser sujeto de la acción. Si no es un ser humano, no puede ser considerar delito.

FASES DE LA ACCIÓN:

• Fase interna. En la fase interna la acción solo sucede en el pensamiento.

• Fase externa. Acá es donde se desarrolla la acción.

Si no hay Fase externa no hay delito.

EL RESULTADO:

El resultado como elemento de la acción que solo se da, que solo se existe en los delitos materiales.

El resultado es el efecto externo de la acción que el Derecho Penal califica para reprimirlo y el ordenamiento jurídico tipifica para sancionarlo que consiste en la

modificación verificable introducida por la conducta en el mundo exterior (por ejemplo robo, incendio) o en el peligro de que dicha alteración se produzca (por ejemplo abandono de niños).

Es un efecto de modificación verificable del mundo exterior trascendente en el ámbito penal.

LA TIPICIDAD:

Adecuación del acto humano voluntario ejecutado por el sujeto a la figura descrita por la ley como delito. Es la adecuación, el encaje, la subsunción del acto humano voluntario al tipo penal. Si se adecua es indicio de que es delito. Si la adecuación no es completa no hay delito.

"La tipicidad es la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la ley penal".

La adecuación debe ser jurídica, no debe se una adecuación social. Como ejemplo de esta última podemos citar: invitar una copa a servidor público (cohecho) o golpes en el boxeo (lesiones). Estos se estiman comportamientos adecuados socialmente, no deben considerarse típicos y mucho menos antijurídicos ni penalmente relevantes.

La TIPIFICACION PENAL es la criminalización de una norma de cultura realizada por el legislador y establecida en una ley penal.

La tipicidad lo aplica el juez, la tipificación lo realiza el legislador- La CALIFICACION de un comportamiento como delito lo hace el fiscal.

CATEGORÍAS DEL TIPO:

Graves. Este tipo establece delitos graves con sanciones penales también agravadas, por ejemplo el asesinato, el parricidio.

Menos graves. Las sanciones son menos graves, por ejemplo la sanción para el homicidio es más corta que para el asesinato.

Leves. Las consecuencias jurídicas son leves. Por ejemplo el castigo para el dolo.

ELEMENTOS DEL TIPO:

Subjetivos. Son características y actividades que dependen del fuero interno del agente, son tomados en cuenta para describir tipo legal de la conducta por eso estos elementos tienen que probarse.

Precisamente las alocuciones: “El que a sabiendas...”, “El que se atribuya autoridad...” que usa el código penal para describir tipos delictivos, aluden a los elementos subjetivos de los mismos. Se debe probar que sabía, se debe probar que actuó como autoridad, etc.

Normativos. Están en:

- Cuando el legislador considera y describe conductas que deben ser tomados como delitos.

- Cuando el juez examina el hecho para establecer su adecuación al tipo penal respectivo.

Objetivos. Son los diferentes tipos penales que están en la Parte Especial del código penal y que tienen como punto de arranque una descripción objetiva de determinados estados y procesos que deben constituir base de la responsabilidad criminal.

Constitutivos. Sujetos (activo y pasivo), conducta y objetos (material, jurídico).

ANTIJURICIDAD:

Antijuridicidad. Es el acto voluntario típico que contraviene el presupuesto de la norma penal, lesionando o poniendo en peligro bienes e intereses tutelados por el Derecho. La antijuridicidad es un juicio impersonal objetivo sobre la contradicción existente entre el hecho y el ordenamiento jurídico.

La condición o presupuesto de la antijuridicidad es el tipo penal. El tipo penal es el elemento descriptivo del delito, la antijuridicidad es el elemento valorativo. Por ejemplo el homicidio se castiga sólo si es antijurídico, si se justifica como por un Estado De Necesidad como la legítima defensa, no es delito, ya que esas conductas dejan de ser antijurídicas aunque sean típicas.

ANTIJURIDICIDAD FORMAL Y MATERIAL:

La Antijuridicidad Formal es la violación de la norma penal establecida en el presupuesto hipotético de la ley penal que no encuentra amparo en una causa de

justificación de las que el código penal expresamente recoge. Por ejemplo el estado de necesidad (la legítima defensa, el hurto famélico, etc.

La Antijuridicidad Material es la lesión o puesta en peligro de un bien jurídico por una conducta antisocial y dañosa, aunque no siempre tipificada en los códigos penales. Por ejemplo la mendicidad que es un peligro porque puede generar robos.

El ordenamiento jurídico penal boliviano se guía por el Principio de antijuridicidad formal.

Doctrinalmente se discute si la antijuridicidad tiene carácter objetivo o subjetivo, se sigue la Teoría de que la antijuridicidad es objetiva porque es una oposición entre la conducta humana y las reglas del Derecho positivo. Estas dos últimas son objetivas.

ANTIJURIDICIDAD GENÉRICA Y ESPECÍFICA:

Genérica se refiere al injusto sin precisarlo en sus peculiaridades. Específica, es aquella en que lo injusto está referido a una descripción especifica de un delito.

ANTIJURIDICIDAD Y TIPICIDAD:

El tipo tiene carácter descriptivo, la tipicidad, encaje, subsunción (al tipo), la antijuridicidad es valorativa.

Para la Escuela Clásica, el delito es un acto contrario a la ley, esto es, atendía al elemento descriptivo de la infracción. Modernamente el delito viola la norma penal,

no en sí la ley penal; por eso la conducta debe ser valorada ante la norma. De ahí que delitos iguales en su revestimiento son valorados de distinta manera, por ejemplo en dos homicidios, si uno de ellos es en legítima defensa deja de ser antijurídico.

La valoración es sobre la conducta desarrollada del sujeto (valoración objetiva), se valora el impulso volitivo no el contenido de la voluntad, esta última es valorada subjetivamente dentro la culpabilidad.

LÍMITE DE LA ANTIJURIDICIDAD: LA TIPICIDAD

Si decimos que la antijuridicidad es la conducta humana contraria al ordenamiento jurídico, tendríamos con esta afirmación una antijuridicidad genérica, para delimitar se apela al tipo, con lo que se tiene una antijuridicidad específicamente penal.

LA IMPUTABILIDAD:

Capacidad psíquica de una persona de comprender la antijuridicidad de su conducta y de no adecuar la misma a esa comprensión. Se es imputable o no. No hay términos medios.

Pero algunas veces un sujeto deja de ser imputable por las llamadas Causas De Inimputabilidad (Situaciones que, si bien la conducta es típica y antijurídica, hacen que no sea posible atribuir el acto realizado al sujeto por no concurrir en él: salud mental, conciencia plena, suficiente inteligencia o madurez psíquica; que son:

Enfermedad mental. Denominación general para toda perturbación mental mayor de origen orgánico y/o emocional, caracterizada por pérdida de contacto con la realidad, a menudo con alucinaciones e ilusiones. En las psicosis existe alteración de la inteligencia, en las psicopatías hay alteración de la personalidad.

Grave Insuficiencia de la Inteligencia. La oligofrenia (del griego "oligo", poco y "prhéen", inteligencia) es un síndrome neurológico caracterizado por déficit intelectual congénito o precozmente adquirido.

Grave Perturbación de la conciencia. Situación en que se encuentra el sujeto cuando sufre una alteración de la percepción de la realidad. Puede ser causado por una embriaguez alcohólica, o puede tener origen en la sordomudez y ceguera de nacimiento

Ser menor de 16 años. Las disposiciones del Código Penal, se aplicaran a las personas que en el momento del hecho fueren mayores de dieciséis años. A los menores no se les aplica una pena, sólo una medida de seguridad.

LA CULPABILIDAD:

La Culpabilidad es la Situación en que se encuentra una persona imputable y responsable, que pudiendo haberse conducido de una manera no lo hizo, por lo cual el juez le declara merecedor de una pena. Es la situación en que se encuentra una persona imputable y responsable. Es una relación de causalidad ética y psicológica entre un sujeto y su conducta.

La culpabilidad tiene dos formas: el dolo y la culpa. La primera es intención, la segunda, negligencia. Ambas tienen por fundamento la voluntad del sujeto activo. Sin intención o sin negligencia no hay culpabilidad, y sin ésta, no hay delito, por ser la culpabilidad elemento del delito.

LA PENALIDAD:

La penalidad para algunos es elemento del delito. La penalidad se traduce en una sanción que es la pena.

La pena (del latín "poena", sanción) Privación o disminución de un bien jurídico a quien haya cometido, o intente cometer, un delito.

Toda conducta típica antijurídica y culpable es punible por regla, excepto cuando:

Existe excusas absolutorias, ej., leyes de perdón.

No hay condición objetiva de punibilidad, p. ej., el autor debe ser mayor de 18 años, sino solo se le aplica una medida de seguridad.

No hay condición de perseguibilidad, p. ej., en la violación de mujer mayor de edad, necesita demanda.

La causa de la pena es el delito cometido. La esencia, es la privación de un bien jurídico. El fin es evitar el delito a través de la prevención general o especial.[3]

---

[3] *RANIERI, Silvio Derecho Penal: Teoría del Delito, México, 1997.*

LA ESTAFA.

En forma general se conoce que cometen estafa los que con ánimo de lucro, utilizando engaño para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno, o también según se observa en el Diccionario Jurídico Espasa sostiene que en España se consideran "reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero"

Para que se considere estafa deben existir varias circunstancias que en algunos países se tipifica en forma expresa y en otros países como el nuestro en cambio se lo hace en forma muy general permitiendo que cuando se defienda el infractor invocando el principio de que no hay castigo sin ley previa, los delitos de estafa informática se quedan en la impunidad.[4]

LA PERSONA.

En el lenguaje cotidiano, la palabra persona hace referencia a un ser con poder de raciocinio que posee conciencia sobre sí mismo y que cuenta con su propia identidad. El ejemplo excluyente suele ser el hombre, aunque algunos extienden el concepto a otras especies que pueblan este planeta.

---

[4] *DICCIONARIO JURÍDICO ESPASA, España, 2001*

En el ámbito del derecho, una persona es todo ente que, por sus características, está habilitado para tener derechos y asumir obligaciones. Por eso se habla de distintos tipos de personas: personas físicas (como se define a los seres humanos) y personas de existencia ideal o jurídica (grupo donde se agrupan las corporaciones, las sociedades, el Estado, las organizaciones sociales, etc.).

Las personas físicas o naturales están contempladas desde un concepto de naturaleza jurídica que fue elaborado por juristas romanos. En la actualidad, las personas físicas cuentan, por el solo hecho de existir, con diversos atributos reconocidos por el derecho.

Las personas jurídicas o morales son aquellos entes que, para llevar a cabo ciertos propósitos de alcance colectivo, están respaldados por normas jurídicas que les reconocen capacidad para ser titulares de derechos y contraer obligaciones.[5]

Definiciones de persona en el Derecho.

Entre las innumerables definiciones de persona en Derecho, podemos citar tres, todas equivalentes: 1° Persona es todo ente susceptible de tener derechos o deberes jurídicos. 2° Persona es todo ente susceptible de figurar como término subjetivo en una relación jurídica; y, 3° Persona es todo ente susceptible de ser sujeto

[5] *http://definicion.de/persona/*

RELACIÓN ENTRE EL CONCEPTO DE PERSONAS Y OTROS CONCEPTOS.

Conviene distinguir y señalar las relaciones entre el concepto de persona y los conceptos de personalidad, capacidad jurídica o de goce, sujeto de derecho y cosa.

1° Persona, personalidad y capacidad jurídica o de goce. Persona es el ente apto para ser titular de derechos o deberes jurídicos, personalidad es la cualidad de ser persona, o sea, la aptitud para ser titular de derechos o deberes jurídicos. De allí que en el lenguaje ordinario se diga que se es persona y que se tiene personalidad.

Muchos autores consideran como sinónimas las expresiones personalidad y capacidad jurídica o de goce; pero, en sentido estricto, personalidad es la aptitud dicha, y capacidad jurídica o de goce es la medida de esa aptitud. De allí que pueda decirse que la personalidad no admite grado (simplemente se tiene o no se tiene), mientras que la capacidad sí (puede ser mayor en una persona que en otra.

2° Persona y sujeto de derecho. Si se entiende por sujeto de derecho aquel que actualmente tiene un derecho o deber, el concepto de persona es más amplio porque comprende también a quien puede llegar a tener un derecho o un deber, aunque actualmente no lo tenga. Pero tomada la expresión, "sujeto de derecho" en abstracto, o sea sin referirla a ningún derecho o deber concreto, viene a ser sinónimo de persona.

3° Persona y cosa. A las personas, o sea, a los posibles sujetos de derecho, se contraponen las cosas, las cuales sólo pueden llegar a ser objetos de derechos. Entre esas cosas no se incluyen en la actualidad a los seres humanos. En cambio, la expresión comprende tanto las llamadas cosas corporales, como las incorporales.[6]

4.2. MARCO DOCTRINARIO.

EL DELITO INFORMÁTICO.

“Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Para Carlos Sarzana, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

María de Luz Lima dice que el "delito electrónico" en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

---

[6] *http://www.monografias.com/trabajos24/concepto-personas/concepto-personas.shtml*

De los conceptos anotados podemos deducir elementos comunes: la computadora como medio o fin de la infracción; y, el uso de la informática para el cometimiento de la conducta delictiva.

Por lo tanto, resumiendo, diremos que delitos informáticos son aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Como todo delito, el informático tiene un sujeto activo y otro pasivo:

SUJETO ACTIVO: En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computación.

SUJETO PASIVO: en el caso del delito informático pueden ser: individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información."[7]

Los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y

[7] */articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/el-delito-informatico.*

culpables que tienen a las computadoras como instrumento o fin" (concepto típico).[8]

TIPOS DE DELITOS INFORMÁTICOS.

"Clasificación según el "Convenio sobre la Ciberdelincuencia" de 1 de Noviembre de 2001.

Con el fin de definir un marco de referencia en el campo de las tecnologías y los delitos para la Unión Europea, en Noviembre de 2001 se firmó en Budapest el "Convenio de Ciberdelincuencia del Consejo de Europa". En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos:

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

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos.
- Interferencia en el funcionamiento de un sistema informático.
- Abuso de dispositivos que faciliten la comisión de delitos.

Algunos ejemplos de este grupo de delitos son: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger.

---

[8] *RANIERI, Silvio Derecho Penal: Teoría del Delito, México, 1997.*

Delitos informáticos:

- Falsificación informática mediante la introducción, borrada o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

El borrado fraudulento de datos o la corrupción de ficheros algunos ejemplos de delitos de este tipo

Delitos relacionados con el contenido:

Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:

- Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática.

Con el fin de criminalizar los actos de racismo y xenofobia cometidos mediante sistemas informáticos, en Enero de 2008 se promulgó el “Protocolo Adicional al Convenio de Ciberdelincuencia del Consejo de Europa” que incluye, entre otros aspectos, las medidas que se deben tomar en casos de:

- Difusión de material xenófobo o racista.

- Insultos o amenazas con motivación racista o xenófoba.
- Negociación, minimización burda, aprobación o justificación del genocidio o de crímenes contra la humanidad.

Clasificación según la página de la Brigada de Investigación Tecnológica de la Policía Nacional Española (www.policia.es/bit/index.htm)

Ataques que se producen contra el derecho a la intimidad:

Delito de descubrimiento y revelación de secretos mediante el apoderamiento y difusión de datos reservados registrados en ficheros o soportes informáticos. (Artículos del 197 al 201 del Código Penal)

Infracciones a la Propiedad Intelectual a través de la protección de los derechos de autor:

Especialmente la copia y distribución no autorizada de programas de ordenador y tenencia de medios para suprimir los dispositivos utilizados para proteger dichos programas. (Artículos 270 y otros del Código Penal)

Falsedades:

Concepto de documento como todo soporte material que exprese o incorpore datos. Extensión de la falsificación de moneda a las tarjetas de débito y crédito. Fabricación o tenencia de programas de ordenador para la comisión de delitos de falsedad. (Artículos 386 y ss. del Código Penal)

Sabotajes informáticos:

Delito de daños mediante la destrucción o alteración de datos, programas o documentos electrónicos contenidos en redes o sistemas informáticos. (Artículo 263 y otros del Código Penal)

Fraudes informáticos:

Delitos de estafa a través de la manipulación de datos o programas para la obtención de un lucro ilícito. (Artículos 248 y ss. del Código Penal)

Amenazas:

Realizadas por cualquier medio de comunicación. (Artículos 169 y ss. del Código Penal)

Calumnias e injurias:

Cuando se propaguen por cualquier medio de eficacia semejante a la imprenta o la radiodifusión. (Artículos 205 y ss. del Código Penal)

Pornografía infantil:

Entre los delitos relativos a la prostitución al utilizar a menores o incapaces con fines exhibicionistas o pornográficos.

La inducción, promoción, favorecimiento o facilitamiento de la prostitución de una persona menor de edad o incapaz. (art 187)

La producción, venta, distribución, exhibición, por cualquier medio, de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, aunque el material tuviere su origen en el extranjero o fuere desconocido. (art 189). La posesión de dicho material para la realización de dichas conductas. (art 189).”[9]

TIPOS DE DELITOS INFORMÁTICOS RECONOCIDOS POR LAS NACIONES UNIDAS.

DELITOS	CARACTERÍSTICAS
Fraudes cometidos mediante manipulación de computadoras	
Manipulación de datos de entrada	Este tipo de fraude informático, conocido también como *de los datos sustracción de datos,* representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. No requiere conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de éstos.
DELITOS	**CARACTERÍSTICAS**
Manipulación de Programas de Computadoras	Es muy difícil descubrirla y a menudo pasa inadvertida debido a que el delincuente ha de tener conocimientos técnicos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado caballo de Troya, el cual consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
Manipulación de datos de salida	Para efectuarla se fija un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, pero en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las Tarjetas bancarias y las de crédito.
Fraude efectuado por manipulación informática	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salami”, en la cual "rodajas muy finas", apenas perceptibles, de transacciones financieras se sacan repetidamente de una cuenta y se transfieren a otra.

[9] *http://www.delitosinformaticos.info/delitos_informaticos/tipos_delitos.html*

Falsificaciones Informáticas	
Como objeto	Cuando se alteran datos de los documentos almacenados en forma computarizada.
Como instrumentos	Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en colora base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución. Modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los auténticos
Daños o modificaciones de programas o datos computarizados	
Sabotaje informático	Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: virus, gusanos, y bomba lógica o cronológica, los cuales se detallan a continuación.
Virus	Es una serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como mediante el método del caballo de Troya.
Gusanos	Se fabrican de forma análoga al virus con miras a infiltrarlos en programas legitimas de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos, podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita
DELITOS	**CARACTERÍSTICAS**
Bomba lógica o cronológica	Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en un futuro. Ahora bien, a diferencia de los virus o de los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos Informáticos criminales, son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente, La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla
Falsificaciones Informáticas	
Acceso no autorizado a sistemas o servicios	Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hacker) hasta el sabotaje o espionaje informático
Piratas informáticos o heckers	El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación, El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para tener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder en aquellos sistemas en los que los usuarios pueden emplear contraseñas comunes o de mantenimiento que están en el sistema
Reproducción no autorizada dé programas informáticos de protección legal	Ésta puede entrañar una pérdida económica sustancial para los propietarios legítimas. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico por tutelar es la propiedad intelectual

Fuente: *RANIERI, Silvio Derecho Penal: Teoría del Delito, México, 1997.*

PORNOGRAFÍA INFANTIL EN INTERNET

La palabra pornografía se deriva de pornógrafo (del griego πορνογ, prostituta, y préfijo de escritura), y se define como el carácter obsceno de obras literarias o artísticas, A su vez, el concepto de obscenidad está referido a lo impúdico u ofensivo al pudor.

Debido a que el carácter de lo que es obsceno se vincula con las variantes culturales que existen en el mundo, el concepto de pornografía infantil difiere también conforme a las prácticas de comportamiento sexual, las creencias religiosas y los valores morales que tiene cada sociedad.

Dicha situación motiva que tanto la definición como las medidas que establecen los distintos países en sus legislaciones para evitar la pornografía infantil tengan alcances diferentes.

En el ámbito internacional, la Convención sobre los Derechos del Niño adoptada por Naciones Unidas en 1989 establece una referencia a la pornografía infantil, al mencionarla como forma de explotación y abuso sexual, contra la que deberá protegerse a los niños como compromiso de los Estados miembros.

Posteriormente, en 2000, el Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, define a la pornografía infantil como "toda representación, por cualquier medio, de un niño dedicado a actividades sexuales

explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales".

En el Convenio sobre Cibercriminalidad del Consejo de Europa de 20013 se da Una definición más amplia que incluye el material en sistemas informáticos: "La pornografía infantil comprende todo material pornográfico que represente de manera visual: a) a un menor dedicado a un comportamiento sexualmente explícito; b) a alguien que parezca un menor dedicado a un comportamiento sexualmente explícito, y e) imágenes realistas que representen a un menor dedicado a un comportamiento sexualmente explícito."

El uso masivo de internet ha propiciado un crecimiento exponencial de la pornografía infantil debido a la facilidad para dar visibilidad, publicidad y acceso a todo tipo de materiales.

Internet hace factible la Consulta de páginas web con material pornográfico, pero mantiene al usuario en el anonimato. Los programas "peer to peer" hacen posible compartir el material ubicado en el disco duro de las computadoras, sin dejar rastro. El correo electrónico permite enviar fotografías o videos de una punta del mundo a la otra en cuestión de segundos, sin correr el riesgo de pasar por aduanas o controles policiales. Los chats, foros y páginas de comunidades facilitan la comunicación entre pedófilos e incluso el contacto directo con menores.

El uso más actual y novedoso es lo que se ha dado en llamar pornografía virtual, que consiste en la creación de contenidos sexuales con imágenes no reales, como

dibujos y animaciones de menores. Esto suscita un hondo debate y provoca problemas al perseguir la pornografía infantil legal y judicialmente porque no existen las personas ni las situaciones reproducidas; a pesar de ello, fomenta el consumo de otros materiales que sí lo hacen.[10]

LA ESTAFA INFORMÁTICA.

"La estafa informática es una fenómeno delictivo que en los últimos años está tomando mayor magnitud y relevancia en el ámbito de la criminalidad informática, siendo éste la base principal del delito informático sobre el que gira la ciberdelincuencia.

A pesar de las diferencias que existen a la hora de establecer una definición unitaria del concepto de estafa informática y/o fraude informático (concepto éste más apropiado según la doctrina), debemos entender que nos referiremos a éstos como "la producción de un daño patrimonial cuantificable mediante un comportamiento externo, impropio de un proceso automatizado informático, que altera los datos gestionados por éste, con ánimo lucro y en perjuicio de tercero". Por su parte, el Código penal establece a aquella conducta, "con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, que consiga la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero".

---

[10] *RANIERI, Silvio Derecho Penal: Teoría del Delito, México, 1997.*

Los elementos típicos que integran el delito de estafa informática son:

- La manipulación informática y artificio semejante,
- Transferencia patrimonial no consentida por el titular del mismo,
- Ánimo de lucro, y
- Perjuicio en tercero.

El concepto de **manipulación informática** puede definirse como la introducción, alteración, borrado o supresión indebida de datos informáticos, especialmente datos de identidad, y la interferencia ilegítima en el funcionamiento de un programa o sistemas informáticos, cuyo resultado sea la transferencia no consentida de un activo patrimonial en perjuicio de tercero. Por tanto, queda incluido en el término la introducción de datos falsos, la introducción indebida de datos reales, la manipulación de los datos contenidos en el sistema, así como las interferencias que afectan al propio sistema.

La **transferencia de un activo patrimonial** consiste en el traspaso fáctico de un activo; esto es, una operación de transferencia de un elemento patrimonial valorable económicamente que pasa del patrimonio originario a otro, no teniendo necesariamente que producirse por medios electrónicos o telemáticos.

El ánimo de lucro es elemento subjetivo del injusto que consiste en el propósito o intención del delincuente de conseguir un beneficio o ventaja económica.

El actor de la estafa informática deberá actuar en **perjuicio de tercero,** el cuál sufre un daño en su activo patrimonial, dando así lugar a la consumación del delito."[11]

[11] *http://portaley.com/2012/12/introduccion-a-la-estafa-informatica-2/*

4.3. MARCO JURIDICO.

PROTECCIÓN DE LA PERSONA, POR PARTE DEL ESTADO.

EL ART. 3 "Que son deberes primordiales del Estado;

1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación y en los instrumentos internacionales, en particular la salud, la educación, la seguridad social y el agua para sus habitantes"[12]

Las personas son sujetas de derechos, por lo que el Estado por medio de la ley mantiene un orden interno observando la buena conducta, y principios para garantizar la eficacia de sus derechos.

Las normas penales deben garantizar la eficacia de la protección de forma integral de los derechos legalmente constituidos a fin de que no se los menoscabe o conculque, o lesione por falta de ley.

El Art. 424.-"La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica.

---

[12] *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. 2008*

La Constitución y los instrumentos internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público."[13]

La constitución de la república del Ecuador, garantiza un marco de legal a través de la ley, lo que garantiza el derecho a la vida, como un bien jurídico dentro de los preceptos constitucionales. Éstos regulan la vida de un estado y garantiza los bienes jurídicos a todos y cada una de las personas que forman parte de la sociedad, a fin de mantener un correcto control social.

El Art. 425.-"El orden jerárquico de aplicación de las normas será el siguiente:

La Constitución; los tratados y convenios internacionales; las leyes orgánicas; las leyes ordinarias; las normas regionales y las ordenanzas distritales; los decretos y reglamentos; las ordenanzas; los acuerdos y las resoluciones; y, los demás actos y decisiones de los poderes públicos.

En caso de conflicto entre normas de distinta jerarquía, la Corte Constitucional, las juezas y jueces, autoridades administrativas y servidoras y servidores públicos, lo resolverán mediante la aplicación de la norma jerárquica superior. La jerarquía normativa considerará, en lo que corresponda, el principio de competencia, en especial la titularidad de las competencias exclusivas de los gobiernos autónomos

---

[13] *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. 2008*

descentralizados. El Estado se somete a la jurisdicción interna, para garantizar el respeto de los derechos de las personas, de la misma manera que garantiza la vigencia de los derechos fundamentales de las personas, y por ende cumple con los convenios, pactos y tratados internacionales de los cuales es signatario. En materia de derechos y garantías Constitucionales, todas las personas deben cumplirlos, y especialmente las instituciones del Estado por consiguiente, no se puede vulnerar los derechos de las personas, o desconocer los derechos que ellas tienen.[14]

EL DELITO INFORMÁTICO EN LA CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR.

El bien jurídico protegido al tipificar y penalizar la estafa informática como delito autónomo, es la propiedad; y la Constitución se refiere al derecho a la propiedad en la siguiente norma:

"Art. 66.- Se reconoce y garantizará a las personas:

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

---

[14] *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. 2008*

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

26. El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas"[15]

La carta constitucional, reconoce a los ciudadanos su derecho a la protección de sus datos, es decir, nadie puede invadir la vida privada de los individuos; el derecho a la propiedad constitucionalmente, debe aplicarse este principio constitucional en las leyes, de manera tal que se garantice en forma efectiva la tipificación y penalización de nuevas formas delictivas

LA ESTAFA INFORMÁTICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL ECUATORIANO.

DELITOS CONTRA LA SEGURIDAD DE LOS ACTIVOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN[16]

---

[15] *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. 2008*

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.

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 un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes

---

[16] Código Integral Penal (COIP)

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 a la que quiere acceder.

3. 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.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

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

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos. La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

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

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

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

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

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

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.

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

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

Art. 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.

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.

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. [17]

El Ecuador ha iniciado una nueva etapa legislativa, relacionado con los fraudes informáticos, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, que de alguna forma llena el vacío legal que se generó y que permite asegurar que no queden en la impunidad los actos que se cometan relacionados con las tecnologías; lo que ocasiona la violación de los derechos constitucionales de las personas víctimas de estos delitos.

---

[17] *COIP Oficio No. SAN-2014-0138 Quito, 03 de febrero de 2014*

LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), publicada en el Registro Oficial Suplemento # 337 del 18 de mayo del 2004, fue expedida con la finalidad de llevar a la práctica la disposición contenida en el Art. # 81 de la Constitución Política de 1998, en la que disponía qué "la información es un derecho de las personas que garantiza el Estado".

Artículo 1.- "El acceso a la información pública es un derecho de las personas que garantiza el Estado.

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG's), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley".

La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional

(estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, bajo este mismo contexto las disposiciones contenidas en la Constitución de la República del Ecuador, en su capítulo tercero de las Garantías Jurisdiccionales de sus secciones cuarta y quinta de los Art. 91 y 92 sobre la acción de acceso a la información pública y acción de Habeas Data, también se establece dichas garantías.

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos fue publicada en el Registro Oficial N° 557 del 17 de Abril del 2002 en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos.

Artículo 1.- "Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas".

Artículo 57.- "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley".

La Ley contiene los principios jurídicos que regirán la generación, difusión y comunicación de los mensajes de datos, se le concede pleno valor y eficacia

jurídica a los mensajes de datos, tanto a su información como a su contenido general. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable.

LEY ORGÁNICA DE GARANTÍAS JURISDICCIONALES Y CONTROL CONSTITUCIONAL.

Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, fue publicada en el Registro Oficial N° 52 del 22 de Octubre del 2009.

Artículo 49.- "La acción de habeas data tiene objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informe que por sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos".

En la Constitución de la República del Ecuador, en su capítulo III. En relación a las Garantías Jurisdiccionales de su sección quinta Art. 92, también se establece el recurso jurídico de Habeas Data.

4.4. LEGISLACIÓN COMPARADA.

COMPARACIÓN DEL DELITO INFORMATICO EN EL DERECHO.

EN FRANCIA:

En Francia la Ley Nro 88-19, relativa al Fraude Informático de 1992, introdujo el Capítulo II al libro II del Título II del Código Penal, bajo la denominación “De ciertas infracciones en materia informática” Esta Ley fue modificada por la Ley 92-683 de 1992, que traslado las disposiciones informáticas al Libro II, Título II Capítulo III. De los atentados contra los sistemas de tratamiento automatizado de datos.

El legislador francés utilizó la técnica legislativa especial, esto es, la conducta la criminalizó por medio de una disposición penal, o juego de disposiciones de la misma clase, castigando las especialidades de un particular uso indebido, o abuso informático. Así, ha introducido los llamados delitos informáticos, mediante la tipificación, artículo por artículo, de determinadas acciones que ha sido objeto de sanción penal; la supresión, modificación y alteración de los datos contenidos en un sistema informático, trabar o falsear el funcionamiento del sistema; suprimir o modificar el modo de tratamiento o de la transmisión de los datos, falsificación de documentos informáticos. Sin embargo, las defraudaciones patrimoniales por medios informáticos quedan sin una específica regulación, siendo cubiertas por un articulado que amplió el concepto de documentos incluyendo el electrónico, cuidando eso sí, de que no se lesione derechos fundamentales como el de la

legalidad, y eso subraya Muñoz de Alba, al indicar que es evidente que las tecnologías de información, junto con la telemática, le da al derecho de información una proyección ilimitada. De ahí la importancia de que los avances científicos y tecnológicos, así como las figuras jurídicas que los regulen, estén destinados a servir al ciudadano y no a atentar contra la identidad humana, ni contra los derechos del hombre, ni contra la vida privada, ni contra las libertades individuales y públicas (Estos son los artículos consagrados en el Artículo 1ro de la Ley francesa Nro. 78-17 del 6 de Enero de 1978, relativa a la informática, los ficheros y libertades).- Y encontramos un buen argumento en el pensamiento de Ferrajoli: en el primer sentido (lato) el principio de legalidad se identifica con la reserva relativa de ley, entendiendo "ley" en el sentido formal de acto o mandato legislativo, y se limita a prescribir la sujeción del juez a las leyes vigentes, cualquiera que sea la formulación de sus contenidos, en la calificación jurídica de los hechos juzgados. En el segundo sentido (estricto) se identifica en cambio con la reserva absoluta de ley, entendiendo ley, en el sentido sustancial de norma o contenido legislativo; y prescribe además que tal contenido esté formado por supuestos típicos dotados de significado unívoco y preciso, por lo que es posible su empleo como figuras de cualificación en proposiciones judiciales verdaderas o falsas y resulta así garantizada la sujeción del juez solamente a la ley.

Según los autores investigados, probablemente ha sido Alemania, el país donde se ha ponderado con especial cuidado la conveniencia político-criminal de penalizar determinadas conductas relativas a la informática, queriendo colmar una laguna legal inaplazable, según había denunciado la doctrina alemana. Las

modificaciones efectuadas por la Segunda Ley para la Lucha contra la Criminalidad Económica, de 1986, en el Código Penal previendo las conductas delictuales relacionadas con los medios informáticos, no sólo consistieron en la modificación de algún precepto ya existente, en los que se agregaron las palabras datos, registros o almacenamiento, sino que introdujeron una serie de nuevos tipos penales relativos a la delincuencia informática: el espionaje de datos, estafa mediante ordenador o fraude informático, falsificación de datos probatorios.

EN ITALIA:

El legislador estableció las disposiciones sobre delito informático en el Código Penal, usando la técnica legislativa de la extensión esto es, elaboró una figura especial, paralela e inspirada en otras existentes, pero con relación a bienes nuevos como los sistemas informáticos, los datos y el software, y con nueva formulación de actos o acciones que proceden o son propios del ámbito informático. Se cubre el nuevo modus operandi a través de actos delictivos tradicionales.

ARGENTINA:

Dispone un anteproyecto completo de delitos informáticos considerando que la información, como valor a proteger, ha sido tenida en consecuencia por el Derecho Penal en otras ocasiones. Sin embargo, se lo ha hecho desde la óptica de la confidencialidad, pero no como un nuevo bien jurídico tutelado abarcativo de varios intereses dignos de protección penal. Según estudios, la respuesta es que

el Código Penal argentino (con 77 años de vida) no tiene reglas específicas sobre delitos cometidos a través de computadoras. Esto es así porque cuando se sancionaron las leyes no existía la tecnología actual y por tanto no fueron previstos los ataques actuales.

Carlos Parma, en el Código Penal de la Nación Argentina comentado, nos trae jurisprudencia de Virus Informático en el que básicamente se resalta a un ataque a través de mensajes electrónicos infectados con virus efectivamente puede haber sido afectada una empresa, logrando interrumpirla su línea de producción, lo que sin duda causa pérdida de tiempo y un consecuente perjuicio económico pero que de ninguna manera se verifica un daño de tipo tutelado y la reparación de aquel debe ser resultado mediante la vía civil, ajena al Derecho Penal.

CHILE:

Chile tiene una ley relativa a los delitos informáticos que la van renovando de manera constante; y, el delito informático, es considerado como aquella acción típica, antijurídica y culpable realizada por medios informáticos o cuya acción busque modificar los datos de un dispositivo informático, concepto que trata de englobar la perspectiva informática; implicando el concepto generalizado de delito e incluyendo el uso del medio informático o su modificación, de esta manera, engloba las dos acciones que se ejecutan al cometer este tipo de delitos; se utiliza el medio o se busca modificar (entendiendo modificar como transformar o cambiar algo, de esta manera, este verbo engloba cualquier aspecto de alteración, daño etc., que ocurra en el dispositivo informático).

PERU:

Perú cuenta también con una ley de delitos informáticos, y Colombia, en el mes de enero celebró dos años de entrada en vigencia de la Ley de delitos Informáticos, aunque a criterio de Díaz García, se excluyeron tipos tan importantes como la falsedad informática, el spam, y le modificaron el epígrafe a la estafa informática por transferencia no consentida de activos.

COSTA RICA:

En Costa Rica, crecen día a día los delitos de este tipo. Este país creó la Unidad de Delitos Informáticos de Organismos de Investigación Judicial en el año 1996, fecha a partir del cual y hasta el año 2001, habían recibido alrededor de 300 casos, un promedio de 60 casos cada año, según se informa en varios artículos publicados en la prensa nacional.

EL SALVADOR:

En el Salvador se ven limitado los procesos de investigación de delitos informáticos, porque no cuenta con suficiente personal capacitado en el uso de evidencia digital, según Portillo, La Fiscalía General de la República y la Corte Suprema de Justicia presentan debilidades, ya que no tienen leyes en las cuales se puedan amparar para juzgar a individuos detenidos y procesados para cometer delitos informáticos. Además, las instituciones encargadas de preparar profesionales en informática no han abordado el tema de la informática forense, debido a la falta de personal capacitado para impartir conocimientos sobre dicha temática.

ESPAÑA:

En España se dispone de un marco legal regulado para los ámbitos penal, civil, y laboral. El código Penal español (modificado por LO 15/2003: Efectos 1-10-2004, citado por Cifuentes Mateos, menciona que pese a no existir un título específico sobre “Delitos Informáticos” en las categorías de tipos penales se ubican la utilización de medios informáticos y contra medios informáticos y describe los delitos contra:

- La confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. (hacking)
- Delitos Informáticos (Falsificación y fraudes).
- Delitos relacionados con el contenido (pedofilia, amenazas, racismo…)
- Delitos relacionados con infracciones de la propiedad intelectual y derechos ajenos.

La protección de datos personales sin duda, constituye una prioridad jurídica estructurada inicialmente bajo la conceptualización de un derecho fundamental denominado Hábeas Data, que funciona para que no se comparta la información íntima y para que esta información pueda corregirse, actualizarse o modificarse en todo momento, acción que se puede, intentar solamente por su titular argumenta Hernández Delgado, resumiendo que se requiere intensificar la protección jurídica en torno a los datos personales, bajo mecanismos que van desde la protección legal en los procesos de capacitación, almacenamiento, sistematización y modos de compartirla, hasta los mecanismos legales para conocer datos propios y

modificarlos cuando son imprecisos o erróneos. Expone que algunos aspectos normativos actuales se relacionan con la intimidad y complementan su noción protectora, entre ellos destacan la inviolabilidad domiciliaria, la inviolabilidad de comunicaciones y el derecho a la propia imagen, cada uno de ellos estructura sus propios bienes jurídicos tutelados y la forma de ejercitarlos. Que las nuevas tecnologías de la información también inciden en el tema de producción segura la información personal sistematizada y que ello ha obligado al avance normativo en torno a materias como contratos informáticos o electrónicos, flujo de datos transfronterizos, comercio electrónico, gobierno electrónico y delitos informáticos, por lo que resulta innecesario implementar un mecanismo de protección jurídica en torno a los datos personales, bajo un procedimiento que asegure su ejercicio y que permita acceder a la información personal de la que cada individuo es titular y que además asegure la forma jurídica para cambiarla cuando así se requiera.

Una de las novedades más significativas del Código Penal Español a criterio de Borrallo, fue lo incluido en el ya por sí novedoso y confuso capítulo Primero “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio” este precepto castiga con las mismas penas que establece el número Uno, esto es, prisión de uno a cuatro años…, en primera instancia, el apoderamiento, la utilización o la modificación, sin estar autorizado y en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos, o en cualquier otro tipo de fichero o registro público o privado.

5. MATERIALES Y MÉTODOS.

MATERIALES.

Para el desarrollo del presente trabajo investigativo, se demandó de los siguientes materiales:

Materiales bibliográficos:

- Libros
- Internet
- Folletos
- Revistas

Materiales de escritorio:

- Empastados y anillados
- Computadora
- Esferográficos
- Cuadernos de notas
- Hojas de papel bond
- Flash memory
- Calculadora

MÉTODOS.

MODALIDAD BÁSICA DE LA INVESTIGACIÓN.

Para desarrollar la presente investigación, se utilizaron métodos, procedimientos y técnicas de investigación científica, que permitirán el desarrollo de la investigación.

Bibliográfico – Documental.

En la investigación, se obtuvo información de fuentes secundarías, obtenidos a través de libros, textos, módulos, periódicos, revistas jurídicas, así como de tesis disponibles.

Linkográfico.

La investigación, a más de contar con información bibliográfica y documental, se basó en información digital obtenida a través de las páginas de internet.

De campo.

De recabó información al lugar donde se genera los hechos, a través de encuestas a profesionales del derecho en libre ejercicio, consideradas en la presente investigación.

MÉTODO CIENTÍFICO.

El método científico es un proceso cuyo objetivo es establecer vínculos entre los hechos, enunciando leyes que expliquen los fenómenos del mundo y permitan obtener, conocimientos útiles para los individuos sociales.

Método empleado con la finalidad de producir nuevas ideas, partiendo de conceptos y razonamientos para crear juicios, descubrir elementos que componen la totalidad en un proceso de análisis de aspectos, situaciones, ideas, hechos particulares, para llegar al principio o ley general que los determina.

METODO INDUCTIVO

El método inductivo es aquel método científico que alcanza conclusiones generales partiendo de hipótesis o antecedentes en particular.

Es un proceso analítico, el cual parte de estudio de casos, hechos o fenómenos particulares para llegar al descubrimiento de un principio o ley general que lo rige.

Método que permitió obtener, describir, principios generales de la Legislación Ecuatoriana aplicado a sanción de cada uno de los delitos informáticos, en base al análisis de los diferentes casos particulares observables.

METODO DEDUCTIVO.

En este método se desciende de lo general a lo particular, de forma que partiendo de enunciados de carácter universal y utilizando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo cuando las premisas de partida la constituyen axiomas (proposiciones no demostrables), o hipotético-deductivo si las premisas de partida son hipótesis contrastables.

Método que permitió presentar un conjunto de afirmaciones usado para describir los delitos informáticos actuales, que servirá de base para deducir conclusiones y consecuencia de cada delito.

MÉTODO SINTÉTICO.

Es un proceso mediante el cual se relaciona hechos aparentemente aislados y se formula una teoría que unifica los diversos elementos. Consiste en la reunión racional de varios elementos dispersos en una nueva totalidad, este se presenta más en el planteamiento de la hipótesis. El investigador sintetiza las superaciones en la imaginación para establecer una explicación tentativa que someterá a prueba.

Mediante éste método, se pudo definir y conocer los delitos informáticos generados y su tratamiento judicial de los mismos.

TÉCNICAS.

Como técnicas de investigación para la recolección de la información utilizaremos la, entrevista y la encuesta.

LA ENTREVISTA.

Técnica que permitió a recopilar datos e información de 30 profesionales de la abogacía en libre ejercicio y que tienen relación con la temática a investigar, y que se levantará a información a través de un banco de preguntas previamente elaboradas, en donde se registrará sus opiniones.

LA ENCUESTA.

La encuesta, consiste en formular una serie de preguntas, referentes a un tema específico; la encuesta es una forma de sondeo inmediato, investiga la opinión pública respecto del grado de aceptación o rechazo en distintos temas.

En la presente investigación, se realizará 30 encuestas a ciudadanos comunes, en la que obtendrá información con respecto a su percepción de los delitos informáticos y sobre la vulnerabilidad de sus derechos constitucionales.

6. RESULTADOS.

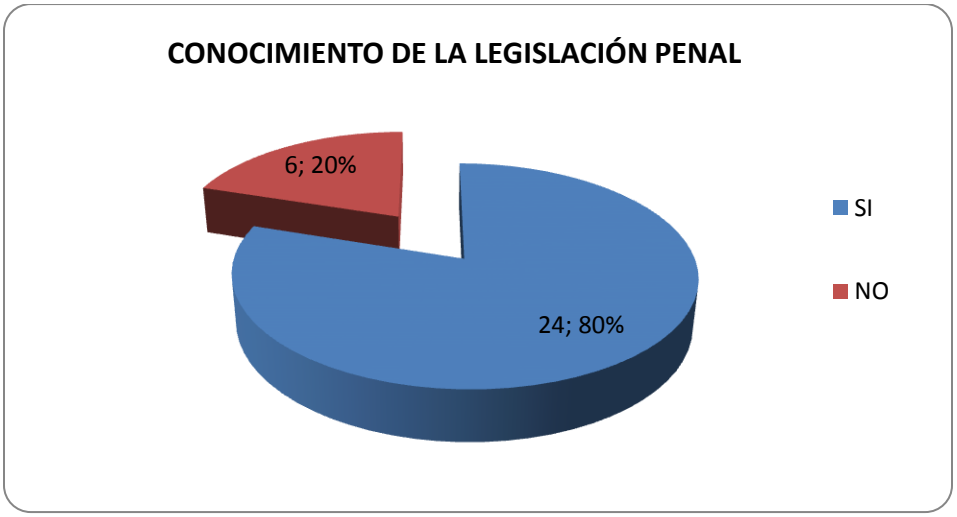
Para efectos de cumplir con los objetivos propuestos, y alcanzar los requerimientos metodológicos establecidos en la Carrera de Derecho, de la Modalidad de Estudios a Distancia, se realizó el trabajo investigativo de campo a través de la aplicación de la técnicas de la entrevista a veinte en libre ejercicio profesional y a veinte ciudadanos comunes, cuyos resultados se presentan utilizando cuadros estadísticos y gráficos que permiten visualizar de mejor forma los resultados obtenidos, para luego analizarlos e interpretarlos.

RESULTADOS DE LA ENCUESTA A PROFESIONALES DEL DERECHO.

1. ¿Conoce usted si en la Legislación Penal establece sanciones para el delito informático, cuando se afecta nuestros derechos personales en lo relacionado a la moral y las buenas costumbres?

Cuadro y Gráfica No. 1 Conocimiento de la legislación penal.

Indicador	Frecuencia	Porcentaje
SI	24	80%
NO	6	20%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

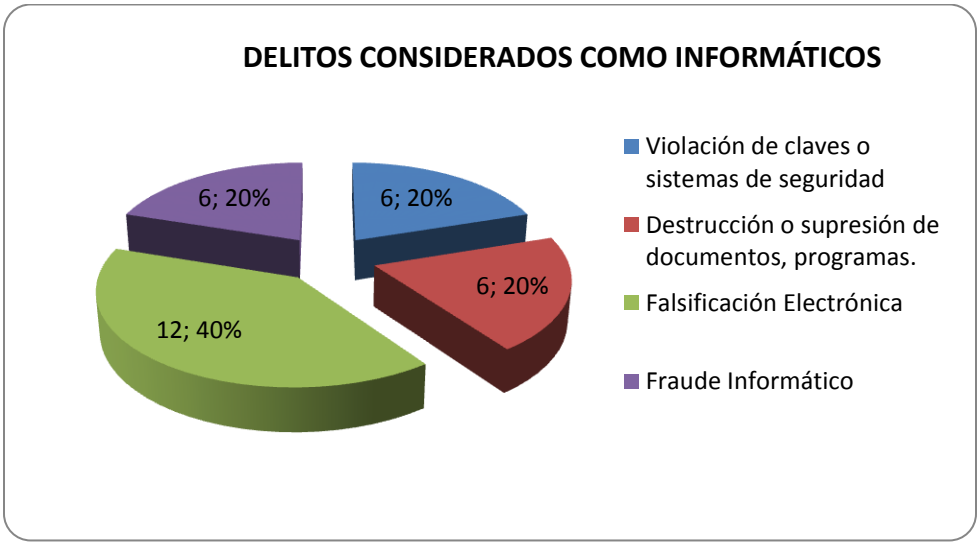
De las 30 Abogados entrevistados, 24 que corresponde al 80%, manifestaron que si conocen la sanción para este tipo de delitos que afecta a los derechos de las personas, mientras que de los entrevistados que corresponde al 20% manifestaron que no conocen las sanciones para este tipo de delitos informáticos.

Los resultados de esta pregunta, demuestra que existe una gran disparidad en cuanto al delito informático, el mismo que causa daño a las personas y que debe ser castigado drásticamente.

2. Según su experiencia profesional, de los siguientes delitos considerados como informáticos, cual es el que con mayor frecuencia se denuncia:

Cuadro y Gráfica No. 2 Delitos considerados como informáticos

Indicador	Frecuencia	Porcentaje
Violación de claves o sistemas de seguridad	6	20%
Destrucción o supresión de documentos, programas.	6	20%
Falsificación Electrónica	12	40%
Fraude Informático	6	20%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz..

ANALISIS E INTERPRETACIÓN:

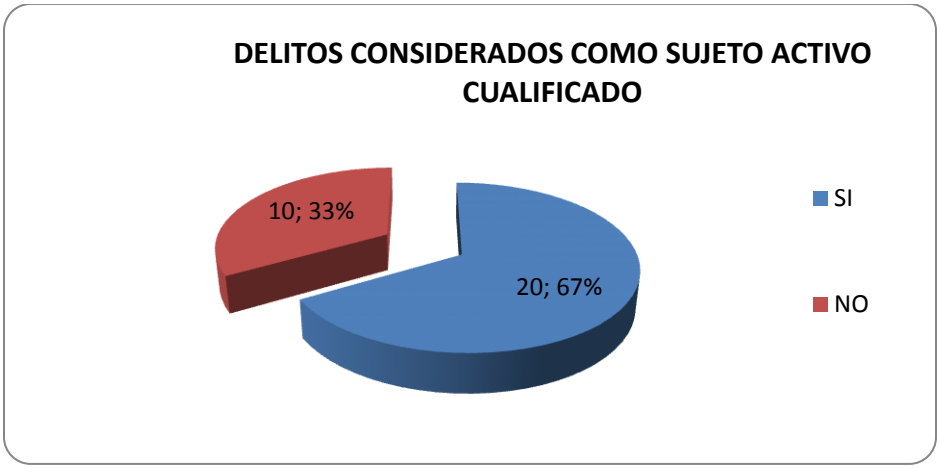
De los 30 Abogados entrevistados, 6 que corresponden al 20% del universo, señalan que el delito informático que con mayor frecuencia se denuncia es el de violación de claves o sistemas de seguridad; así mismo 6 entrevistados que igualmente representan el 20% de los entrevistados, señalan que es la destrucción o supresión de documentos o programas, mientras que 12 abogados entrevistados que representan el 40% del universo encuestado, señalan que es la falsificación electrónica, el delito mayormente denunciado por la ciudadanía; y, finalmente 6 entrevistados que representan también el 20% indican que es el fraude informático el delito informático que mayormente se comete y en consecuencia el más denunciado.

El criterio de la mayoría de los profesionales entrevistados, tiene relación con los adelantos tecnológicos de la época, pues es la falsificación electrónica el delito de moda en nuestro país. Entre estos delitos, están los relacionados con el uso de su ingenio para sustraer datos de tarjetas de crédito, débito, etc., para posteriormente con esa información falsificar estos instrumentos y emplearlos en beneficio personal.

3 ¿Está usted de acuerdo en que los delitos informáticos están revestidos de algunos elementos constitutivos como dolo y sujeto activo cualificado?

Cuadro y Gráfica No. 3 Delitos considerados como sujeto activo cualificado.

Indicador	Frecuencia	Porcentaje
SI	20	67%
NO	10	33%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

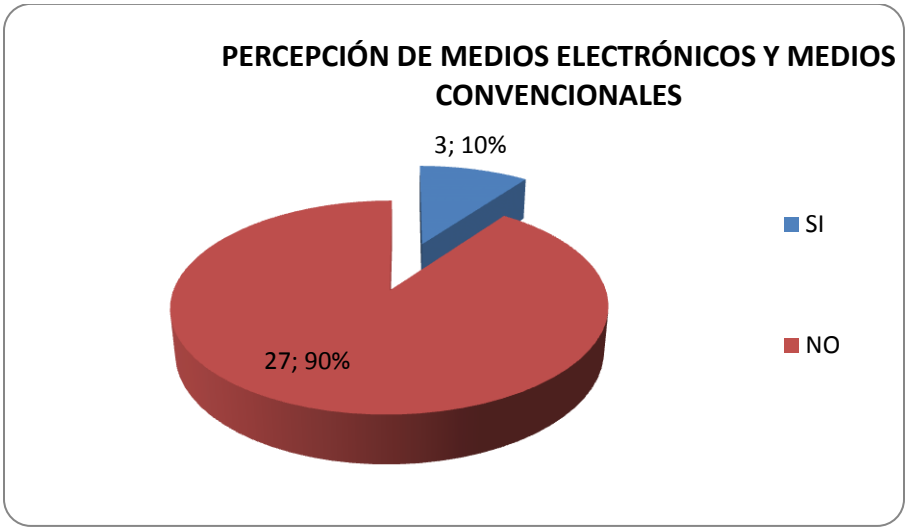
De los 30 Abogados entrevistados, 20 que corresponden al 67% del universo, señalan que los delitos informáticos tienen como principales elementos constitutivos al dolo, el sujeto activo cualificado; y, 10 de los entrevistados no consideran como elementos constitutivos al dolo, el sujeto activo cualificado.

El criterio mayoritario de los entrevistados, tiene congruencia, ya que al perpetrar un delito de esta naturaleza se requiere tener conocimiento previo y además conocimientos en informática.

4. ¿Cree Ud., que las transacciones efectuadas mediante medios electrónicos brindan más seguridad que las realizadas por medios convencionales?

Cuadro y Gráfica No. 4 Percepción de medios electrónicos y medios convencionales

Indicador	Frecuencia	Porcentaje
SI	3	10%
NO	27	90%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 abogados entrevistados, 3 que corresponden al 10% del universo, señalan que las transacciones efectuadas mediante medio electrónicos brindan mayor seguridad que las realizadas convencionalmente; mientras que 27 profesionales, que representan el 90% indican que este tipo

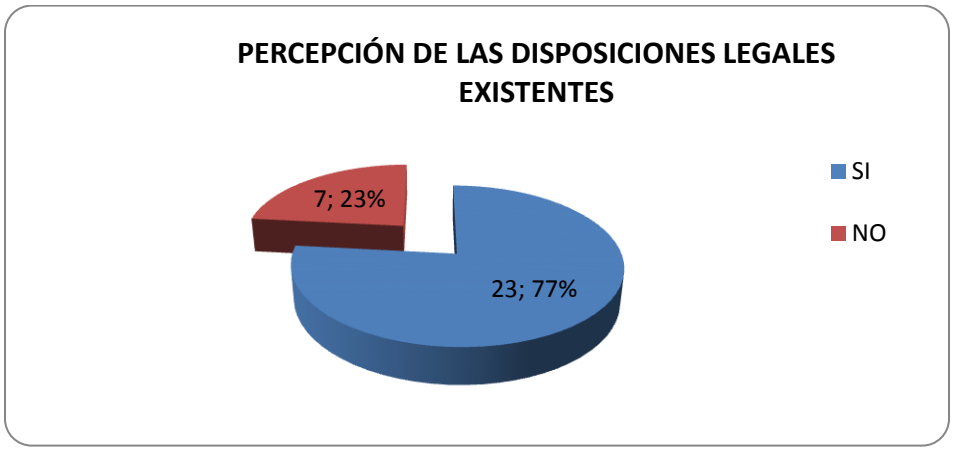
de transacciones no brindan mayores seguridades que las que ofrece una transacción convencional.

Este resultado encontrado, tiene su explicación, por las creencias y dogmas de seguridad que se tiene en la sociedad ecuatoriana, ya que el medio que se elija para efectuar una transacción, no es el problema, pues siempre estaremos expuestos a que alguna persona de mala fe perjudique a otra, empleando cualquier artimaña. A esto debe sumarse el problema es la corrupción que está enraizada en nuestra sociedad; pero mientras existan más medios electrónicos a través de los cuales se realicen toda clase de transacciones, nuestras leyes deben garantizar nuestros derechos e ir a la par con los adelantos tecnológicos.

5. ¿Considera usted que las disposiciones legales que regulan la falsificación electrónica en nuestro medio, son suficientes?

Cuadro y Gráfica No. 5 Percepción de las disposiciones legales existentes.

Indicador	Frecuencia	Porcentaje
SI	23	77%
NO	7	23%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 abogados entrevistados, 7 que corresponden al 23% del universo, consideran que las disposiciones legales que regulan la falsificación electrónica en nuestro medio son suficientes; mientras que 23 profesionales, que representan el 77%, consideran que las disposiciones legales que regulan la falsificación electrónica en nuestro medio no son suficientes.

Este resultado manifiesta que debe revisarse las disposiciones legales permanentemente, ya que existe un rápido desarrollo de la tecnología y con ello el incremento de los delitos informáticos, a los cuales se debe combatir.

6. ¿Ud., ha sido víctima de violaciones de la privacidad personal con el uso de la informática?

Cuadro y Gráfica No. 6 Victima de violaciones por el uso de la informática.

Indicador	Frecuencia	Porcentaje
SI	12	40%
NO	18	60%
TOTAL	**30**	**100%**

Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 abogados entrevistados, 12 que corresponden al 40% del universo, consideran que han sido víctimas de la privacidad personal con el uso de la

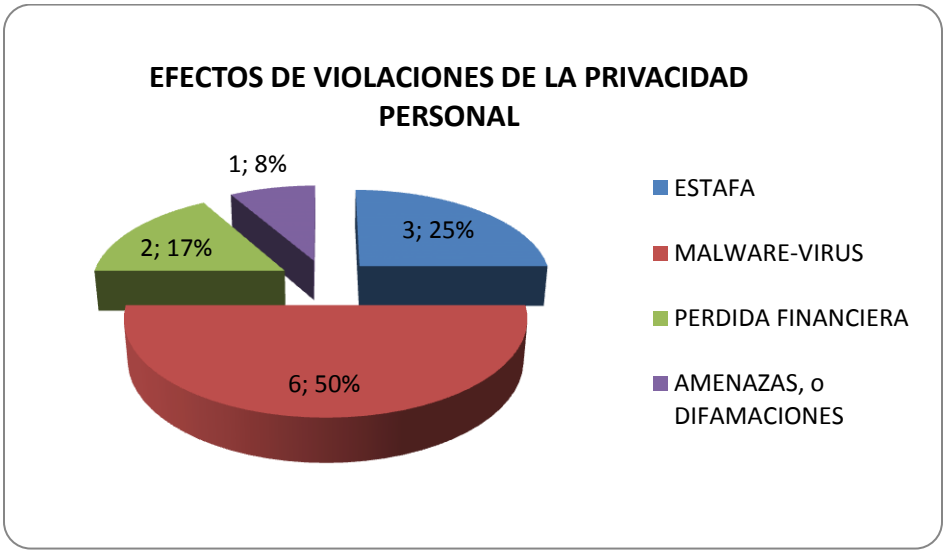
informática; mientras que 18 profesionales, que representan el 60%, consideran que no han sido víctimas de la privacidad personal por el uso de la informática.

Este resultado manifiesta que a pesar que la mayoría de los entrevistados no ha sido víctima de la privacidad personal, puede a futuro encontrarse en esta difícil situación, en la que se está violentando su privacidad.

7. Si la respuesta a la pregunta anterior es si, ¿cuáles fueron los efectos de esas violaciones?

Cuadro y Gráfica No. 7 Efectos de violaciones de la privacidad personal.

Indicador	Frecuencia	Porcentaje
ESTAFA	3	25,0%
MALWARE-VIRUS	6	50,0%
PERDIDA FINANCIERA	2	16,7%
AMENAZAS, o DIFAMACIONES	1	8,3%
TOTAL	**12**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

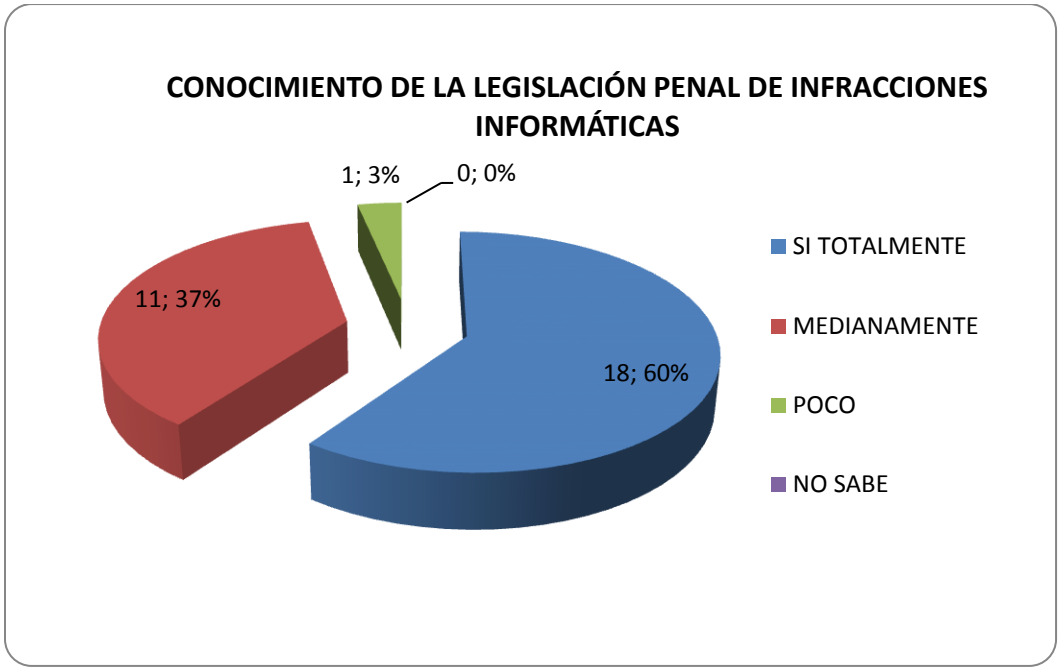
De los 30 abogados entrevistados, 3 de los entrevistados, consideran que fueron víctimas de estafa, que representan el 25%; 6 de los entrevistados fueron víctima de Malware o virus, que representan el 50%; 2 de las personas entrevistadas manifiestan ser víctimas de perdidas financieras, que representan el 16,7% y 1 manifiesta ser víctimas de amenaza o difamación, que representan el 8,3%, constituyendo de esta manera el 100%.

Los resultados manifiestan que en donde más se encontró violación de la seguridad informática y más alto porcentaje en las víctimas de los virus informáticos, debido seguramente por el hecho de descargar programas que esconden detrás de los programas y búsqueda de información.

8. ¿Conoce Ud. las leyes tipificadas en el Código Integral Penal del ecuador, que permitan sancionar las infracciones informáticas?

Cuadro y Gráfica No. 8 Conocimiento de la legislación penal de infracciones informáticas

Indicador	Frecuencia	Porcentaje
SI TOTALMENTE	18	60%
MEDIANAMENTE	11	37%
POCO	1	3%
NO SABE	0	0%
TOTAL	**30**	**100%**



Fuente: Abogados en libre ejercicio.
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 abogados entrevistados, 18 de los entrevistados, que corresponde al 60%, consideran conocer totalmente la leyes tipificadas en el Código Integral Penal, que sancionan las infracciones informáticas; 11 de los entrevistados lo conocen medianamente y representan el 37%; 1 de las personas entrevistadas manifiestan conocer poco y representan el 3%; ningún entrevistado no sabe nada.

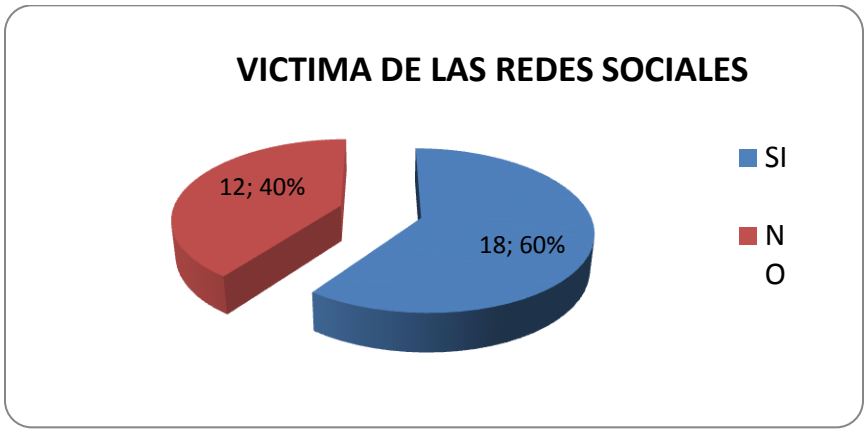
Los resultados indican, que de la muestra de abogados que se efectuó la entrevista, solo el 60% conocen plenamente la legislación de delitos informáticos, y, esto se debe en gran parte por el desconocimiento de la informática.

RESULTADOS DE LA ENCUESTA A CIUDADANOS

1. ¿Usted ha sido víctima de alguna situación en que se hayan apropiado de su información en redes sociales?

Cuadro y Gráfica No. 9 Víctima de vulneración de información en redes sociales.

Indicador	Frecuencia	Porcentaje
SI	18	60%
NO	12	40%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

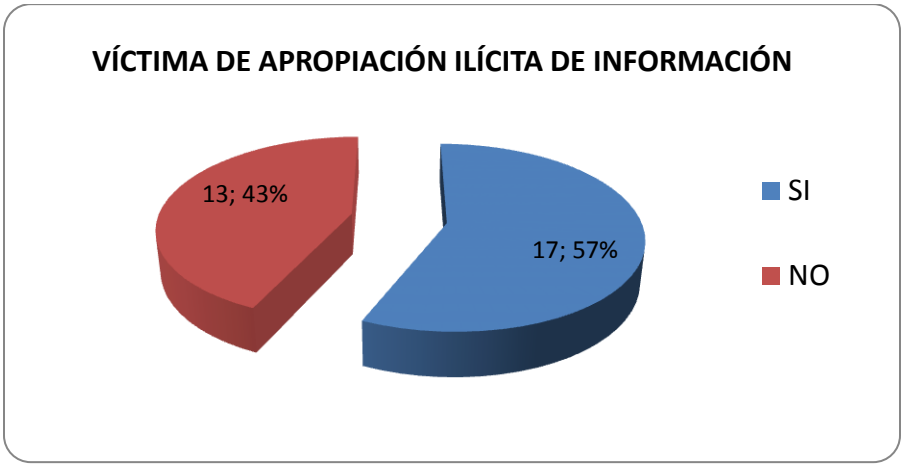
De los 30 ciudadanos encuestados, 18 de los encuestados, que corresponde al 60%, consideran que han sido víctimas de apropiación indebida de la información subida a sus redes sociales; 12 de los encuestados no han sido víctimas de apropiación indebida de la información subida a sus redes sociales.

A pesar de que el 40% ha sido víctima de apropiación de la información en las redes sociales debido al avance de la tecnología informática y el uso de las redes sociales, debe considerarse muy seriamente esta realidad en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

2. ¿Conoce usted de alguna persona que haya sido víctima de apropiación ilícita de su información por medio de las redes sociales?

Cuadro y Gráfica No. 10 Víctima de apropiación ilícita de información.

Indicador	Frecuencia	Porcentaje
SI	17	57%
NO	13	43%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

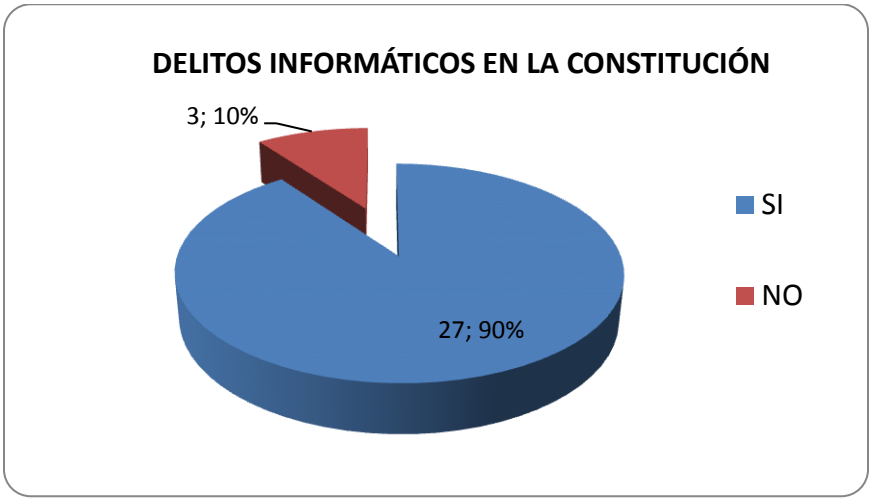
De los 30 ciudadanos encuestados, 17 de los encuestados, que corresponde al 57%, manifiestan conocer de alguna persona que haya sido víctima de apropiación ilícita de su información por medio de las redes sociales; 13 de los encuestados no conocen sobre el particular y que corresponde al 43% de la muestra.

El 57% de los encuestados conocen de alguien que haya sido víctima de apropiación de la información en las redes sociales; esto se justifica por el auge y desarrollo de la tecnología informática y el uso de las redes sociales.

3. ¿Considera usted que los delitos informáticos violan los derechos consagrados en la Constitución?

Cuadro y Gráfica No. 11 Delitos informáticos en la Constitución.

Indicador	Frecuencia	Porcentaje
SI	27	90%
NO	3	10%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 ciudadanos encuestados, 27 de los encuestados, que corresponde al 90%, consideran que los delitos informáticos violan los derechos consagrados en la Constitución; 3 de los encuestados que representan el 10%, no consideran que los delitos informáticos violen los derechos consagrados en la Constitución.

Se debe consideran una realidad de actualidad, que los encuestados afirmaron positivamente, ya que cualquier atentado contra los derechos de cada persona genera de un delito, y particularmente los delitos informáticos que vulneran los derechos consagrados en la Constitución de la República.

4. ¿Cree usted que el derecho a la intimidad se ha visto vulnerado por la apropiación de información que se encuentra en redes sociales y que en muchos casos es personal y familiar?

Cuadro y Gráfica No. 12 Derecho a la intimidad en las redes sociales.

Indicador	Frecuencia	Porcentaje
SI	29	97%
NO	1	3%
TOTAL	**30**	**100%**

Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 ciudadanos encuestados, 29 de los encuestados, que corresponde al 97%, consideran que el derecho a la intimidad se ha visto vulnerado por la apropiación de información que se encuentra en redes sociales y que en muchos casos es personal y familiar; 1 de los encuestados que representan el 3%, no que

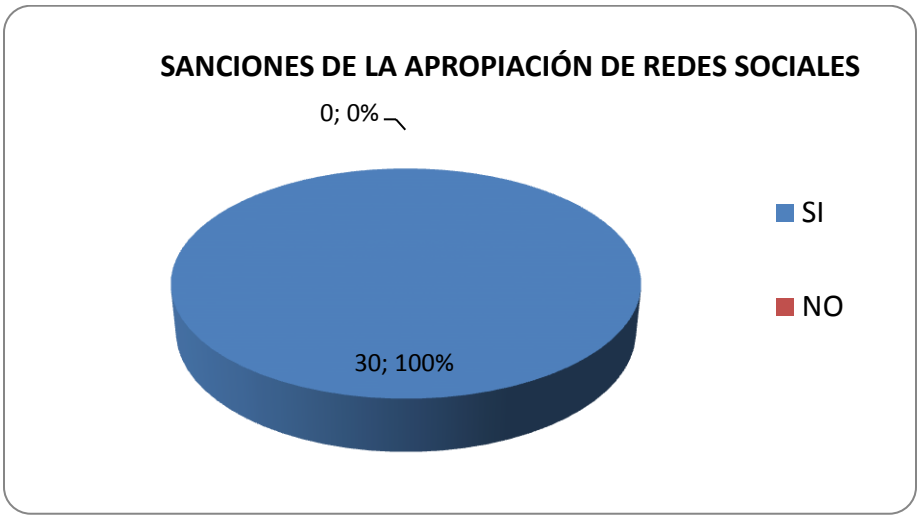
el derecho a la intimidad se ha visto vulnerado por la apropiación de información que se encuentra en redes sociales y que en muchos casos es personal y familiar.

El resultado encuentran que como consecuencia de la apropiación ilícita de su información se ve afectado su derecho a la intimidad, es claro que cualquier delito es atentatorio con los derechos humanos y que debe considerarse esta realidad en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

5. ¿Considera usted que la apropiación ilícita de redes sociales debe tener una sanción en nuestra Legislación Penal?

Cuadro y Gráfica No. 13 Sanciones de la apropiación de redes sociales.

Indicador	Frecuencia	Porcentaje
SI	30	100%
NO	0	0%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

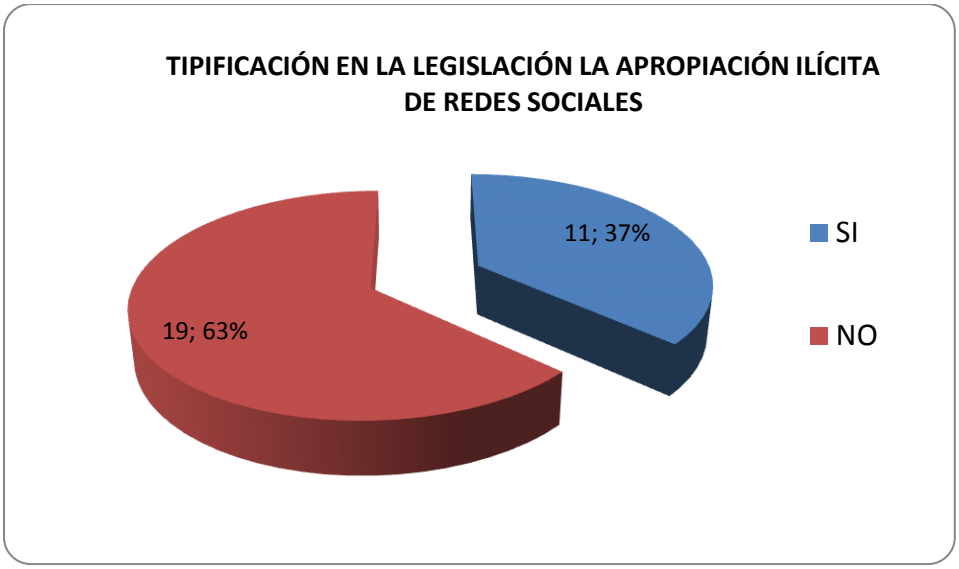
De los 30 ciudadanos encuestados, 30 de los encuestados, que corresponde al 100%, consideran que el que la apropiación ilícita de redes sociales debe tener una sanción en nuestra Legislación Penal. Nadie de los encuestados opina lo contrario.

Con el resultado se puede afirmar que la apropiación ilícita de redes sociales debe tener una pena, es como todo hecho delictivo que cause agravio alguno a una persona debe tener una sanción. En la actualidad en el nuevo Código Orgánico Integral Penal (COIP) promulgado el 3 de febrero de 2014, considera ya penas para los delitos informáticos; sin embargo falta algunos delitos como la apropiación de la información y la intimidad personal.

6. ¿Usted tiene conocimiento, si en el Código Orgánico Integral Penal se encuentra tipificado la apropiación ilícita de redes sociales?

Cuadro y Gráfica No. 14 Tipificación en la legislación la apropiación ilícita de redes sociales.

Indicador	Frecuencia	Porcentaje
SI	11	37%
NO	19	63%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 ciudadanos encuestados, 11 de los encuestados, que corresponde al 37%, tiene conocimiento que en el Código Orgánico Integral Penal se encuentra tipificado la apropiación ilícita de redes sociales; 19 de los encuestados que representan el 63%, no tiene conocimiento que en el Código Orgánico Integral Penal se encuentra tipificado la apropiación ilícita de redes sociales.

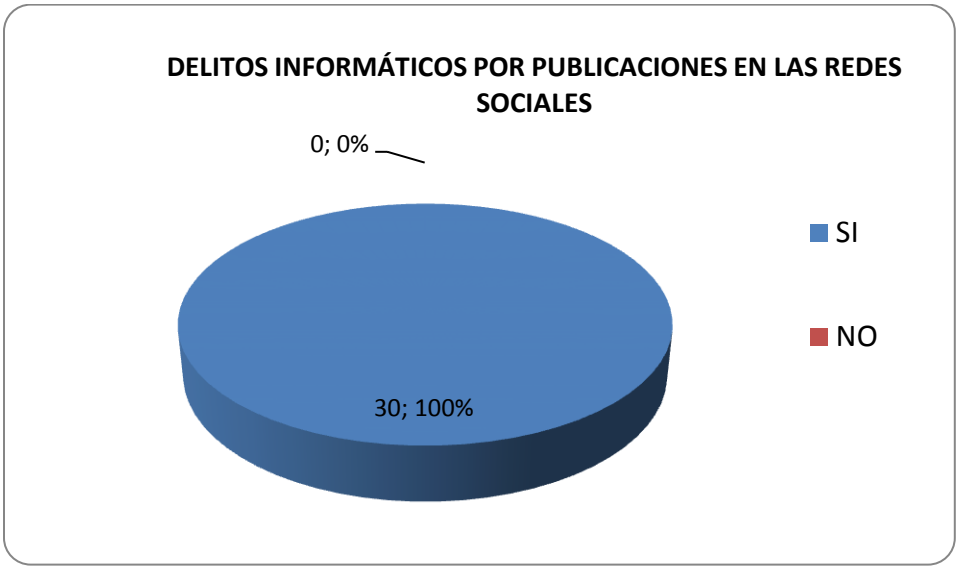
Con el resultado se puede afirmar que la mayoría de los encuestados no tienen conocimiento de la tipificación del delito en el nuevo Código Orgánico Integral Penal.

Sin embargo en el nuevo Código Orgánico Integral Penal (COIP) promulgado el 3 de febrero de 2014, considera ya penas para los delitos informáticos; sin embargo falta algunos delitos como la apropiación de la información y la intimidad personal.

7. ¿Cree usted que al publicar información de sus actividades diarias en redes sociales puede ser víctima de delito informático?

Cuadro y Gráfica No. 15 Delitos informáticos por publicaciones en las redes sociales.

Indicador	Frecuencia	Porcentaje
SI	30	100,0%
NO	0	0,0%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

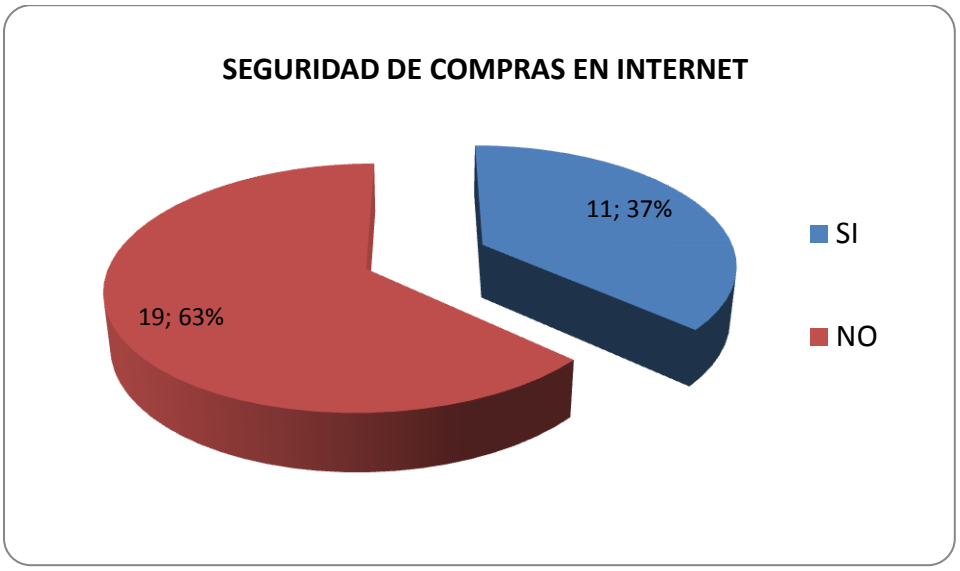
De los 30 ciudadanos encuestados, 30 de los encuestados, que corresponde al 100%, creen que al publicar información de sus actividades diarias en redes sociales puede ser víctima de delito informático. Nadie de los encuestados opina lo contrario.

El hecho de publicar información personal, como fotos, videos, chatear con desconocidos, constituye un peligro para los usuarios de las redes sociales, y a diario se ve en los noticieros sobre atentados, secuestros, etc., debido al mal uso de las redes sociales.

8. ¿Considera Ud., que las compras a través de internet son seguras?

Cuadro y Gráfica No. 16 Seguridad de compras en Internet

Indicador	Frecuencia	Porcentaje
SI	11	37%
NO	19	63%
TOTAL	**30**	**100%**



Fuente: Ciudadanos comunes de la ciudad de Loja
Elaborado por: Carolin Ruiz.

ANALISIS E INTERPRETACIÓN:

De los 30 ciudadanos encuestados, 11 de los encuestados, que corresponde al 37%, consideran que las compras a través de internet son seguras; 19 de los encuestados, que corresponden 63%, consideran que las compras a través de internet no son seguras.

Con el resultado se puede afirmar que la mayoría de los encuestados no tienen conocimiento de la legislación de comercio electrónico.

Es necesario indicar que en el país, mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 577, se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, con la cual se logra se logra regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, logrando un riesgo prácticamente nulo para su falsificación.

7. DISCUSIÓN.

Los resultados de la presente investigación, se desarrolló, de acuerdo a la planificación establecida, cumpliéndose todos los objetivos propuestos, los resultados obtenidos, sirven de base para analizar y conceptualizar la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales; analizar los derechos constitucionales que tiene el ofendido en los delitos informáticos y, permiten establecer las alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

VERIFICACIÓN DE OBJETIVOS.

1. Analizar y conceptualizar la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales.

Para cumplir con la verificación de éste objetivo, se realizó el estudio de la legislación ecuatoriana de las infracciones informáticas estipuladas en el Código Orgánico Integral Penal (COIP) promulgado el 3 de febrero de 2014, relacionadas con la tipificación y sanción, considera para los delitos informáticos.

Por todo lo enunciado anteriormente y en base a todas las consideraciones expuestas ha sido posible la verificación de este objetivo específico.

2. Analizar los derechos constitucionales que tiene el ofendido en los delitos informáticos.

Para cumplir con la verificación de éste objetivo, se realizó el estudio de la legislación ecuatoriana de los derechos constitucionales, consideradas en la Constitución de la República del Ecuador.

Por todo lo enunciado anteriormente y en base a todas las consideraciones expuestas ha sido posible la verificación de este objetivo específico.

3. Establecer alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

En base a las consideraciones expuestas, y de acuerdo a los resultados obtenidos a través de la aplicación de las encuestas, permitió formular una propuesta de código en la COIP.

De acuerdo a la pregunta No. 1 de la encuesta de los profesionales en derecho, los resultados indicaron que existe una gran disparidad en cuanto al delito informático, el mismo que causa daño a las personas y que debe ser castigado drásticamente.

En la preguntas No. 1 de las encuestas a ciudadanos, que debe reformarse la victimización de apropiación de la información en las redes sociales debido al avance de la tecnología informática y el uso de las redes sociales; esta situación debe considerarse muy seriamente esta realidad en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

En la pregunta No. 4, de la encuesta a ciudadanos, se determinó que como consecuencia de la apropiación ilícita de su información se ve afectado su derecho a la intimidad, es necesario que cualquier delito relacionado con los derechos humanos debe considerarse en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

En la pregunta No. 5, y 6, de la encuesta a ciudadanos, se puede afirmar que la apropiación ilícita de redes sociales debe tener una pena, como todo hecho delictivo que cause agravio alguno a una persona debe tener una sanción. En la actualidad en el nuevo Código Orgánico Integral Penal (COIP) promulgado el 3 de febrero de 2014, considera ya penas para los delitos informáticos; sin embargo falta algunos delitos como la apropiación de la información y la intimidad personal.

En la pregunta No. 8, de la encuesta a ciudadanos, se puede afirmar que la mayoría de los encuestados no tienen conocimiento de la legislación de comercio electrónico, por ello es necesario divulgar que mediante Ley No. 67, publicada en el Registro Oficial Suplemento No. 577, se expidió la Ley de Comercio Electrónico,

Firmas y Mensajes de Datos, con la cual se logra se logra regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, logrando un riesgo prácticamente nulo para su falsificación.

8. CONCLUSIONES.

- En la actualidad, la necesidad de comunicación de las personas, ha contribuido al avance vertiginoso de las tecnologías de la información y la comunicación, permitiendo con la misma celeridad los delitos informáticos.

- La necesidad de tipificar y sancionar la apropiación ilícita de la información privada de las personas en las redes sociales, debe ser considerada para precautelar la integridad y la intimidad personas de los ecuatorianos.

- En muchas circunstancias, los delitos informáticos no solo afectan la privacidad de una persona, sino que pueden afectar a un colectivo en general.

- De los resultados obtenidos en las encuestas y entrevistas existe vacío legal en cuanto a la tipificación del delito informático, como la apropiación de la información y la intimidad personal en las redes sociales, y debe considerárselo acto antijurídico y ser causa de sanción, debido a que lesiona los derechos constituidos en la Constitución de la República del Ecuador.

- Las redes sociales son un medio de interacción entre personas, que pueden o no compartir los mismos gustos, plataformas que permiten la

comunicación y la información, pero también es un medio para cometer delitos, que son complicados para poder llegar a determinar la responsabilidad del actor del delito.

- La falta de conocimientos de las tecnologías de la información y la comunicación, es la causa principal para que profesionales del derecho y magistrados, y los reformadores de la legislación penal en materia informática, para que se haya obviado algunos elementos que deberían incluirse en la legislación ecuatoriana.

9. RECOMENDACIONES.

- Es necesaria que la legislación penal, en materia de delitos informáticos sea revisada constantemente, debido a que el avance de las tecnologías de la información y la comunicación es acelerado.

- Los ciudadanos, que están en contacto de las tecnologías de la información y la comunicación, como correos electrónicos, chats, transacciones electrónicas y el uso de las redes sociales, deben precautelar su propia seguridad y limitar el acceso a estas plataformas en lugares públicos.

- Debe incluirse en la legislación penal ecuatoriana, la tipificación del delito informático, como la apropiación de la información y la intimidad personal en las redes sociales y debe considerárselo acto antijurídico y ser causa de sanción.

- Si realiza transacciones bancarias en línea, efectué las transacciones bancarias y pagos de servicios desde su hogar por internet, de esa manera evitará exponerse en la calle a los delincuentes.

- Si una persona ha sido víctima de un delito, debe acudir inmediatamente a denunciarlo en las oficinas más cercanas de la Fiscalía General del Estado

o de la Policía Judicial. Recuerde que al denunciar el delito, contribuirá a que la Fiscalía conozca cómo opera la delincuencia y pueda tomar medidas preventivas encaminadas a disminuir la impunidad y criminalidad del país.

9.1. PROPUESTA DE REFORMA.

La reforma al COIP, debe estar enfocada a los siguientes aspectos:

Debe reformarse la victimización de apropiación de la información en las redes sociales debido al avance de la tecnología informática y el uso de las redes sociales; esta situación debe considerarse muy seriamente esta realidad en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

Como la apropiación ilícita de su información se ve afectado su derecho a la intimidad, es necesario que cualquier delito relacionado con los derechos humanos debe considerarse en la legislación ecuatoriana, a fin de sancionar este tipo de delitos informáticos y que aún no están considerados.

La apropiación ilícita de redes sociales debe tener una pena, como todo hecho delictivo que cause agravio alguno a una persona debe tener una sanción. En la actualidad en el nuevo Código Orgánico Integral Penal (COIP) promulgado el 3 de febrero de 2014, considera ya penas para los delitos informáticos; sin embargo falta algunos delitos como la apropiación de la información y la intimidad personal.

La Ley de Comercio Electrónico, Firmas y Mensajes de Datos, se logra regular los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas, logrando un riesgo prácticamente nulo para su falsificación.

10. BIBLIOGRAFIA

Burneo, R. E. (2010). *Derechos y Garantías Constitucionales en el Ecuador, Evolución y Actualidad.* Quito: Corporación de Estudios y Publicaciones.

Caballenas de las Cuevas, G. (2008). *Diccionario Jurídico Elemental.* Buenos Aires: Editrorial Heliasta.

Carpio, D. S. (2013). *El Delito Informático, Prueba pericial informático.* Quito: Jurídica del Ecuador.

Cisneros Baquero, E. A. (2009). *Los delitos informáticos.* Quito: Universidad Simón Bolívar - Ecuador.

FORUM, E. J. (2009). *Régimen Penal. Código Penal.* Quito.

Holguin, J. L. (2011). *Derecho Constitucional Ecuatoriano.* Loja: Universidad Técnica Particular de Loja.

Jorge, B. C. (2010). *Modalidades Delictivas: El fenómeno de la criminalidad en Guayaquil .* Guayaquil: Editorial ONI.

Martinez, J. (2010). *El peritaje Informático y la Evidencia Digital. .* Bogotá: Universidad de los Andes.

Pascale, M. (2009). *Manual de Peritaje Informático.* Montevideo: Fundación de Cultura Universitaria.

PUBLICACIONES, C. D. (2009). *Leyes conexas. Ley Orgánica de Defensa.* Quito.

Ranieri, S. (1997). *Derecho Penal: Teoría del Delito.* Mexico DF: Universidad Nacional Autómata de México.

sn. (2001). *DICCIONARIO JURÍDICO ESPASA.* España: Editorial Libros S.L.U.

Zavala, J. E. (2010). *Derecho Constitucional, Neoconstitucionalismo y Argumentación Jurídica.* Ecuador: Edilex.

CUERPOS LEGALES:

- Constitución de la República del Ecuador
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Código Orgánico Integral Penal (COIP).
- Ley de Propiedad Intelectual
- Ley Especial de Telecomunicaciones
- Ley Orgánica de Control Constitucional
- Código de Procedimiento Civil
- Ley Orgánica de Defensa Del Consumidor

LINKOGRAFÍA.

- http://www.delitosinformaticos.com
- http://www1.lunarpages.com/derechohoy/informatico.htm

- http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2009/05/27/derecho-informatico.
- http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/delitos-informaticos.
- http://www.dspace.espol.edu.ec/bitstream/123456789/5792/5/TESIS%20%20DELITOS%20INFORMATICOS%20EN%20ECUADOR%20Y%20ADMINISTRACION%20DE%20JUSTICIA.pdf

11. ANEXOS.

ANEXO No. 1 PROYECTO DE TESIS.

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

TEMA:

"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"

PROYECTO DE TESIS PREVIO A LA OBTENCIÓN DEL GRADO DE ABOGADA DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA DEL ECUADOR.

AUTORA: Carolin Anabel Ruiz Cruz

CORREO: carito.xoxo@hotmail.com

Loja – Ecuador

2015

1. TEMA.

“ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS”

2. PROBLEMÁTICA.

El derecho y la tecnología en los últimos años contribuyó a que la sociedad de un giro total en el desarrollo de su vida, hoy el uso de la tecnología, se hace indispensable para la sociedad, y esto ha dado como resultado que en el campo del derecho se agregue una nueva ciencia jurídica como es el derecho informático, en efecto la sociedad ha cambiado tanto en los últimos años, que actualmente ya no hablamos de un derecho tradicional; hoy en día podemos considerar al derecho informático como una ciencia jurídica propia y que puede ser estudiada independiente de las otras ciencias jurídicas, por supuesto esta nueva ciencia jurídica no podrá estar aislada de las demás pues esta debe ser estudiada con el apoyo de ciencias jurídicas tradicionales.

Las cifras de los ciberataques son alarmantes en nuestro medio, según Daniel Molina, experto de la empresa Kaspersky, quien asegura que cerca del 16% de usuarios de la región son víctimas de fraudes informáticos, lo cual suma 60’090.173 detecciones de ataques en el 2014. En el Ecuador, sostiene, las cifras podrían ir en aumento debido al crecimiento económico del país, que lo convierte en un blanco interesante para los ataques cibernéticos. “Hay hackers que atacan

desde Perú, Colombia o Europa occidental a los bancos ecuatorianos, lo que antes no sucedía, pues se trata es un delito importado"[18]

Sin embargo, los delitos informáticos, los fraudes informáticos, implican actividades como fraudes, falsificaciones, perjuicios, estafa, sabotaje, haciendo uso indebido de las computadoras; por ello es necesario propiciar su regulación y control en la legislación ecuatoriana.

En materia legal, en el Ecuador en el año 2002 se expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos. Con la expedición de esta Ley, aparecen otros delitos como es el sabotaje (SPAM) y los daños informáticos (CYBER CRIME), estas infracciones se incorporan al Código Penal Ecuatoriano, logrando así una protección concreta y específica a este tipo de actos. La Ley establece que los mensajes de datos electrónicos, tendrán igual valor jurídico que los documentos escritos.

En todo el país y de manera particular en la provincia de Loja, el cometimiento de delitos informáticos, redes sociales, ha lesionado los derechos constitucionales de los ciudadanos, como el derecho a la intimidad personal y familiar que cada individuo posee, el derecho a conservar su patrimonio legalmente adquirido,

---

[18] Diario el Universo Lunes, 17 de noviembre, 2014.

Una de las razones para que los delitos informáticos, vaya en aumento, se debe principalmente a la dificultad de identificar y descubrir a los autores intelectuales, quedando muchos de estos delitos en la impunidad, generando progresivamente que la sociedad pierda la confianza en una justicia eficaz, eficiente y oportuna.

De acuerdo a lo manifestado, es necesario que el estado ecuatoriano, proteja a los mandantes, reformando la legislación ecuatoriana, para identificar la manera adecuada de hacer publicidad política y de esta forma construir una nueva manera del quehacer político en el Ecuador.

Formulación del Problema:

¿Cómo los delitos informáticos violentan y lesionan los derechos constitucionales de los ciudadanos, y en muchos casos, los delitos quedan en la impunidad, por la dificultad de descubrir a los autores?

3. JUSTIFICACIÓN.

El presente trabajo investigativo, se justifica desde los siguientes espacios:

ACADÉMICA.

Como egresada de la Carrera de Derecho, modalidad de estudios a distancia de la Universidad Nacional de Loja, se tiene la facultad y la capacidad de aplicar los conocimientos adquiridos durante la fase de formación en la temática del derecho constitucional ecuatoriano, y a través de la presente investigación alcanzar el

requisito exigido por la normativa universitaria para obtener el título de Abogada de los Tribunales y Juzgados de la república del Ecuador.

El documento que se generará en la presente investigación, será un aporte muy significativo para los estudiantes de las ciencias del derecho.

SOCIAL.

Por la falta de personal investigativo especializado en delitos informáticos se tiene como consecuencia que las personas que cometen estos ilícitos, los delincuentes informáticos, quedan en total impunidad. De tal forma que los perjuicios que se ocasionan a las personas naturales y personas jurídicas de derecho público y privado son de gran magnitud en el Ecuador, por lo que la investigación determina cuáles delitos son sancionados en nuestra legislación y qué ilícitos deben agregarse a la misma. Necesidad manifestada por los requerimientos de los Tribunales de Justicia.

JURÍDICO.

Desde la perspectiva jurídica, la presente investigación propuesta sirve para poder identificar un marco general sobre la conceptualización de las infracciones informáticas, con las regulaciones existentes (leyes) para el manejo de los delitos informáticos, mediante la comprensión de los lineamientos establecidos en nuestra legislación y tener un claro entendimiento de los criterios y medidas contempladas; se pretende además identificar e incorporar nuevos delitos informáticos en la legislación ecuatoriana.

ECONOMICA.

Para la elaboración del trabajo investigativo, se deberá involucrar recursos económicos, los cuáles estoy dispuesto a cubrirlos,

4. OBJETIVOS DE LA INVESTIGACION.

OBJETIVO GENERAL.

Analizar y conocer de manera crítica y jurídica la realidad de los Delitos Informáticos y la violación de los derechos constitucionales de los ciudadanos ecuatorianos.

ESPECÍFICOS.

- Analizar y conceptualizar la naturaleza de las Infracciones Informáticas y sus tipificaciones de acuerdo a sus características principales.
- Analizar los derechos constitucionales que tiene el ofendido en los delitos informáticos.
- Establecer alternativas de soluciones para sancionar los delitos informáticos y evitar la vulneración de los derechos constitucionales del ofendido.

5. HIPÓTESIS.

“La legislación ecuatoriana, no siempre puede sancionar los delitos informáticos en la violación de los derechos constitucionales de los ciudadanos, debido a la dificultad de identificar a los autores con conocimientos avanzados de la informática”.

ANEXO No. 2

ENCUESTA A PROFESIONALES DEL DERECHO EN LIBRE EJERCICIO.

UNIVERSIDAD NACIONAL DE LOJA
MODALIDAD DE ESTUDIOS A DISTANCIA
CARRERA DE DERECHO

Señor Abogado:
Con la finalidad de desarrollar mi tesis del nivel de pre-grado titulada: **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"**, Muy comedidamente le solicito contestar las siguientes preguntas:

1. ¿Conoce usted si en la Legislación Penal establece sanciones para el delito informático, cuando se afecta nuestros derechos personales en lo relacionado a la moral y las buenas costumbres?

Si ( ) No ( )

2. Según su experiencia profesional, de los siguientes delitos considerados como informáticos, cual es el que con mayor frecuencia se denuncia:

Violación de claves o sistemas de seguridad ( )
Destrucción o supresión de documentos, programas. ( )
Falsificación Electrónica ( )
Fraude Informático ( )

3 ¿Está usted de acuerdo en que los delitos informáticos están revestidos de algunos elementos constitutivos como dolo y sujeto activo cualificado?

Si ( ) No ( )

4. ¿Cree Ud., que las transacciones efectuadas mediante medios electrónicos brindan más seguridad que las realizadas por medios convencionales?

Si ( ) No ( )

5. ¿Considera usted que las disposiciones legales que regulan la falsificación electrónica en nuestro medio, son suficientes?

Si ( ) No ( )

6. ¿Ud., ha sido víctima de violaciones de la privacidad personal con el uso de la informática?

Si ( ) No ( )

7. Si la respuesta a la pregunta anterior es si, ¿cuáles fueron los efectos de esas violaciones?

ESTAFA ( )
MALWARE-VIRUS ( )
PERDIDA FINANCIERA ( )
AMENAZAS, o DIFAMACIONES ( )

8. ¿Conoce Ud. las leyes tipificadas en el Código Integral Penal del ecuador, que permitan sancionar las infracciones informáticas?

SI TOTALMENTE ( )
MEDIANAMENTE ( )
POCO ( )
NO SABE ( )

GRACIAS POR SU COLABORACIÓN

ANEXO No. 3

ENCUESTA A CIUDADANOS.

UNIVERSIDAD NACIONAL DE LOJA
MODALIDAD DE ESTUDIOS A DISTANCIA
CARRERA DE DERECHO

Con la finalidad de desarrollar la investigación de mi tesis del nivel de pre-grado titulada: **"ANÁLISIS DE LOS DELITOS INFORMÁTICOS Y SU VIOLACIÓN DE LOS DERECHOS CONSTITUCIONALES DE LOS CIUDADANOS"**, Muy comedidamente le solicito contestar las siguientes preguntas:

Lea detenidamente las preguntas formuladas y marque con una X dentro del paréntesis de la respuesta que usted considere correcta.

1. ¿Usted ha sido víctima de alguna situación en que se hayan apropiado de su información en redes sociales?

   Si ( ) No ( )

2. ¿Conoce usted de alguna persona que haya sido víctima de apropiación ilícita de su información por medio de las redes sociales?

   Si ( ) No ( )

3. ¿Considera usted que los delitos informáticos violan los derechos consagrados en la Constitución?

   Si ( ) No ( )

4. ¿Cree usted que el derecho a la intimidad se ha visto vulnerado por la apropiación de información que se encuentra en redes sociales y que en muchos casos es personal y familiar?

   Si ( ) No ( )

5. ¿Considera usted que la apropiación ilícita de redes sociales debe tener una sanción en nuestra Legislación Penal?

   Si ( ) No ( )

6. ¿Usted tiene conocimiento, si en el Código Orgánico Integral Penal se encuentra tipificado la apropiación ilícita de redes sociales?

   Si ( ) No ( )

7. ¿Cree usted que al publicar información de sus actividades diarias en redes sociales puede ser víctima de delito informático?

   Si ( ) No ( )

8. ¿Considera Ud., que las compras a través de internet son seguras?

   Si ( ) No ( )

GRACIAS POR SU COLABORACIÓN

ÍNDICE