Universidad Nacional de Loja

Facultad Jurídica Social Administrativa

Carrera de Derecho

"Análisis Jurídico y Doctrinario de los Delitos Informáticos Tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal".

Trabajo de Integración Curricular previo a la Obtención del Título de Abogado

AUTOR:

Gabriel Alejandro Cabrera Vivar

DIRECTOR:

Dr. Guilber René Hurtado Herrera, Mg. Sc.

Loja - Ecuador

2024

Certificación

Universidad Nacional de Loja

1859

Sistema de Información Académico Administrativo y Financiero - SIAAF

CERTIFICADO DE CULMINACIÓN Y APROBACIÓN DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, **HURTADO HERRERA GUILBER RENE**, director del Trabajo de Integración Curricular denominado **ANÁLISIS JURÍDICO Y DOCTRINARIO DE LOS DELITOSINFORMÁTICOS TIPIFICADOS EN COLOMBIA, PERÚ Y COSTA RICA PARAINCORPORARLOS AL CÓDIGO ORGÁNICO INTEGRAL PENAL"**, perteneciente al estudiante **GABRIEL ALEJANDRO CABRERA VIVAR**, con cédula de identidad N° **1106046517**.

Certifico:

Que luego de haber dirigido el **Trabajo de Integración Curricular**, habiendo realizado una revisión exhaustiva para prevenir y eliminar cualquier forma de plagio, garantizando la debida honestidad académica, se encuentra concluido, aprobado y está en condiciones para ser presentado ante las instancias correspondientes.

Es lo que puedo certificar en honor a la verdad, a fin de que, de así considerarlo pertinente, el/la señor/a docente de la asignatura de **Integración Curricular**, proceda al registro del mismo en el Sistema de Gestión Académico como parte de los requisitos de acreditación de la Unidad de Integración Curricular del mencionado estudiante.

Loja, 6 de Agosto de 2024

Firmado electrónicamente por:
GUILBER RENE HURTADO HERRERA

F) ----------
DIRECTOR DE TRABAJO DE INTEGRACIÓN CURRICULAR

Certificado TIC/TT.: UNL-2024-002059

1/1

Educamos para Transformar

Autoría

Yo, **Gabriel Alejandro Cabrera Vivar,** declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos, de posibles reclamos o acciones legales, por el contenido del mismo.

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

Firma:

Cédula de identidad: 1106046517

Fecha: Loja, 11 de diciembre de 2024

Correo electrónico: gabriel.cabrera@unl.edu.ec

Teléfono: 0985735049

Carta de Autorización

Yo, **Gabriel Alejandro Cabrera Vivar,** declaro ser el autor del presente Trabajo de Integración Curricular denominado: **"Análisis jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal",** como requisito para optar por el Título de **Abogado**, 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 en el Repositorio Institucional:

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

La Universidad Nacional de Loja, no se responsabiliza por el plagio del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los once días del mes de diciembre del dos mil veinticuatro.

Firma:

Cédula de identidad: 1106046517

Fecha: Loja, 11 de diciembre de 2024

Dirección: Avenida Villonaco y Medardo Ángel Silva

Correo electrónico: gabriel.cabrera@unl.edu.ec

Teléfono: 0985735049

DATOS COMPLEMENTARIOS

Director del Trabajo de Integración Curricular: Dr. Guilber René Hurtado Herrera, Mg. Sc.

Dedicatoria

A mi Dios, que todos los días me protege y me guía por el camino de la verdad. Nunca fue suerte, siempre fue él.

A mi bella madre, mi Cecita, que día a día me aliviaba la vida con sus abrazos y que, con su dulce voz, hizo de los más difícil algo sencillo.

A mi héroe mi papá, Franco Eduardo, que me corrigió cuando estaba equivocado, me motivo todos los días a salir adelante y se sacrificó por darme todo. Con sus enseñanzas, me mostró cómo enfrentar la vida y encontrar soluciones a cualquier problema que se me presente.

A mi hermana, mi Andreina, que siempre ha estado para mí, me escucha y se ríe conmigo, me cuida y se preocupa cuando llego tarde a casa.

A Evelyn, quien desde que tomó mi mano nunca más la soltó, siempre me apoyó y motivó, llenó de luz de mi vida y llenó de amor mi corazón.

Gabriel Alejandro Cabrera Vivar

Agradecimiento

Agradezco a la Universidad Nacional de Loja, a la Facultad Jurídica Social y Administrativa, al director de mi Trabajo de Integración Curricular Dr. Guilber Hurtado, quien, con su conocimiento y profesionalismo, supo brindarme las herramientas necesarias para culminar mi trabajo, del mismo modo, agradezco a la distinguida planta docente por haberme brindado los conocimientos necesarios a lo largo de mi formación profesional.

También, mi más sincero agradecimiento, a mis padres que me enseñaron a esforzarme por lo que deseo y por nunca dejarme solo en este gran camino, y por último gracias a todas aquellas personas que de alguna u otra manera, fueron participes y me aportaron conocimiento para lograr satisfactoriamente, la culminación del presente trabajo de investigación.

"No basta saber, se debe también aplicar. No es suficiente querer, se debe también hacer" **Johann Wolfgang von Goethe**

Gabriel Alejandro Cabrera Vivar

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

1. Título

“Análisis Jurídico y Doctrinario de los Delitos Informáticos Tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal”

2. Resumen

El presente trabajo investigativo titulado “Análisis jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal”, aborda como las legislaciones extranjeras tipifican y sancionan delitos que son cometidos a través las tecnologías de la información y la comunicación, detectando entre ellas los delitos que no han sido objeto de estudio en el Ecuador. El objetivo de este estudio jurídico y doctrinario es como los delitos tipificados en las legislaciones colombiana, peruana y costarricense varían en denominaciones del tipo penal, tipificación de otras conductas, características, y especificaciones de los delitos y penas, asimismo se asemejan en la definición y algunos elementos del delito de los que se encuentran en el sistema legal ecuatoriano. En caso de que se refleje una diferencia notoria, se propone realizar una adecuación de los tipos penales diferentes a nuestro Código Orgánico Integral Penal, presentando una reforma legal para sustentar este problema.

En el desarrollo del mismo se implementó el uso de diferentes métodos y técnicas. Se llevaron a cabo encuestas y entrevistas con profesionales del derecho, especialistas en informática y conocedores del problema; de la misma manera se utilizó métodos como el inductivo, deductivo, hermenéutico y comparativo; además, los resultados muestran que la falta de tipificación de ciberdelitos permite la impunidad de ciertas conductas que no han sido tomadas en cuenta por el legislador y estos actos al ser reflejados en el sistema legal permitirían el ejercicio pleno de los derechos de la ciudadanía, y por último, se destaca la necesidad de una reforma al Código Orgánico Integral Penal para incorporar estos nuevos delitos al mismo.

Este trabajo, destaca la importancia de tomar medidas urgentes contra este tipo de conductas delictivas para de esta manera evitar vacíos legales dentro del sistema penal del país.

Palabras clave: derecho informático, delito informático, estafa informática, reforma legal, facilitación de delito informático.

2.1.Abstract

This research work entitled “Legal and doctrinal analysis of computer crimes classified in Colombia, Peru and Costa Rica to incorporate them into the Comprehensive Organic Criminal Code” addresses how foreign legislation classifies and punishes crimes that are committed through information and communication technologies, detecting among them the crimes that have not been studied in Ecuador. The objective of this legal and doctrinal study is how the crimes classified in the Colombian, Peruvian, and Costa Rican legislation vary in the names of the criminal type, classification of other conducts, characteristics, and specifications of the crimes, and penalties. They also resemble the definition and some elements of the crime found in the Ecuadorian legal system. In case a notable difference is reflected, it is proposed to adapt the different criminal types to our Comprehensive Organic Criminal Code, presenting a legal reform to support this problem. In its development, different methods and techniques were implemented. Surveys and interviews were carried out with legal professionals, computer specialists, and experts on the problem; in the same way, methods such as inductive, deductive, hermeneutic, and comparative were used; in addition, the results show that the lack of a classification of cybercrimes allows the impunity of certain behaviors that have not been taken into account by the legislator and these acts when reflected in the legal system, would allow the full exercise of the rights of citizens. Finally, the need for a reform to the Comprehensive Organic Criminal Code to incorporate these new crimes is highlighted. This work highlights the importance of taking urgent measures against this type of criminal behavior to avoid legal loopholes within the country's criminal system.

Keywords: computer law, computer crime, computer fraud, legal reform, facilitation of computer crime.

3. Introducción

Este trabajo consistió en un "Análisis jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal". Los delitos informáticos, por la realidad en la que vivimos se ha convertido en un asunto de vital importancia y preocupación debido al acelerado crecimiento de estas conductas que afectan derechos como la propiedad, intimidad, privacidad, patrimonio, etc. La presente investigación se centra en analizar este problema desde un estudio jurídico y doctrinario, en donde se definen semejanzas y diferencias en la tipificación de estos tipos penales, además se incluyen los delitos que no son considerados en la ley penal del Ecuador, que se llevan a cabo en el país, y al no estar reflejados en la norma legal, se permite la impunidad de estos hechos.

La parte importante de este tema de estudio se centra en la creciente actividad criminal informática y la falta de regulación jurídica acerca de este tema. El problema planteado es que la no consideración de conductas dentro de la norma penal, permiten que los ciberdelincuentes actúen sin medida y sin consideración contra las personas naturales o jurídicas que son usuarias de este tipo de tecnologías, que, en el contexto actual, es casi la gran mayoría de personas.

Los beneficios de abordar este tema son amplios y de gran validez, ya que se contribuye de manera significativa a la protección de datos, patrimonio y sistemas informáticos, garantizando un libre y seguro acceso a las TIC, en donde las personas pueden gozar libremente de sus derechos. Por otro parte se propone una reforma de la ley penal actual, adaptándola a la realidad tecnológica del país, con el fin de evitar la vulneración de los derechos de la sociedad.

En relación a otros trabajos, esta investigación se basa en estudios previos sobre el tema, integrando conocimientos de diversas áreas doctrinarias y jurídicas para de esta manera poder proporcionar un análisis más comprensivo y detallado. Por ejemplo, el diario el universo refiriéndose a la Policía Nacional del Ecuador nos dice:

> Todas las actividades que contemplen grabaciones y fotografías sin consentimiento o autorización legal, suplantación de claves electrónicas, daños o pérdida de información intencional, intervención o violación en la intimidad de las personas, entre otras, son ilícitas", se indica en el portal de la institución (El Universo, 2021, p. 1).

Esta referencia nos previene a tomar consciencia de que en la realidad actual del Ecuador se puede ser víctima de cualquiera de este tipo de delitos, los cuales en algunas ocasiones se llega a archivar el caso por falta de tipificación de la conducta realizada. Sin embargo, el análisis de

la presente investigación comprendió justamente la falta de tipificación de estas conductas y el agregarlas a la norma jurídica del país para lograr reducir el impacto de estas acciones.

En el presente trabajo investigativo se verificó el objetivo general que consistió en: “Realizar un estudio jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal ecuatoriano”. De igual manera se verificaron los objetivos específicos que se detallan a continuación: primer objetivo específico: “Demostrar que la falta de tipificación y sanción en la legislación penal ecuatoriana de algunas conductas dañosas cometidas mediante medios informáticos permiten la impunidad"; segundo objetivo específico: “Determinar algunas conductas que deben ser tipificadas y sancionadas en el Código Orgánico Integral Penal para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana”; y tercer objetivo específico: “Presentar una propuesta de reforma legal incorporando nuevos delitos informáticos”.

El alcance de este trabajo incluye un análisis jurídico y doctrinal, contemplado con las técnicas de acopio teórico documental, como base para la realización del marco teórico. Sumado a esto realicé un estudio empírico basado en encuestas, entrevistas y un estudio de casos que permitió evidenciar la falta de tipificación y sanción de algunas conductas dañinas en el ámbito informático.

La presente investigación busca resaltar la importancia de estudiar el surgimiento de nuevas conductas delictivas por medios informáticos y sus consecuencias por la falta de regulación jurídica al respecto.

4. Marco Teórico

4.1. Derecho Informático

En la actualidad se puede evidenciar el surgimiento de nuevas tecnologías de la información, nuevos aparatos y dispositivos electrónicos, de igual forma se logra distinguir la gran y beneficiosa evolución que ha logrado el ser humano en las mismas, se ha logrado facilitar muchas actividades en muchos campos como el de la ingeniería, medicina e incluso dentro del hogar. Hoy por hoy, la gran mayoría de las personas tienen una computadora, un teléfono celular o cualquier otro dispositivo electrónico en casa, mismos que son de gran utilidad y beneficio. Pero no todo es bueno, ya que, de igual forma, al surgir beneficios, surgen problemas. Como son nuevas tecnologías, sus problemas son nuevos enigmas a resolver, en el campo jurídico estos problemas han tomado forma y se denominan delitos informáticos, ciberdelitos, delitos cibernéticos o delitos electrónicos. La legislación en el apuro de ir a la par con estas tecnologías, contralando su uso y para contrarrestar el surgimiento de estos nuevos delitos, crea y surge el Derecho informático.

> El derecho informático, como una nueva rama del cocimiento jurídico, es una disciplina en continuo desarrollo, que tiene en su haber (al menos hasta esta fecha) nuevos antecedentes a nivel histórico; empero, podemos decir que las alusiones más específicas sobre esta interrelación existen a partir de 1949 con la obra de Norbert Wiener, en cuyo capítulo 4, dedicado al derecho y las comunicaciones, expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico (Téllez, 2008, p. 8).

Esta acepción, nos hace referencia a que el derecho informático es un concepto totalmente nuevo, a diferencia de las demás ramas del derecho, porque surge recién a mediados del siglo pasado, es necesario aclarar que no surge una mención como tal al concepto de lo que es el Derecho Informático, solo se hace una breve referencia a la relación que existe entre el derecho y las comunicaciones y la influencia existente entre la cibernética con relación al derecho.

Podemos aceptar que el derecho informático es una ciencia nueva y en constante desarrollo porque la ciencia tecnológica y aparatos electrónicos siguen desarrollándose, entonces esta rama del derecho debe desarrollarse de igual manera.

Para una mejor compresión de lo que es Derecho Informático es necesario conocer los diversos conceptos que nos han dado los diferentes estudiosos de la materia.

> Aznit lo define como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el ámbito de la informática y sus derivaciones, especialmente en el área denominada tecnología de la información. El concepto engloba la sociedad de la información, por lo que define una ecuación cuya resultante es el Derecho Informático: derecho + informática + sociedad de la información = derecho informático (Aguilar, 2015, p. 20).

El Derecho Informático se define como un conjunto de reglas que se encargan de normar las consecuencias que surgen en relación a las personas y la informática. La informática se viene a definir como una forma de almacenamiento de información, en la era digital actual, vendría a ser la forma de estudio de técnicas para almacenar y distribuir información electrónica o digital. De esto surgen nuevas relaciones y comportamientos, porque esta información digital en su gran mayoría le pertenece a personas naturales y jurídicas, misma que debe ser protegida por el estado, por ende, el derecho debe acoplarse a estos nuevos surgimientos y debe encontrar la forma de regular los mismos, así aparece el Derecho Informático.

Tenemos también que el jurista Horacio Fernández define al derecho informático como: "El conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática" (Fernández, 2016, p. 1).

Con la aparición del internet, la computadora y más medios electrónicos surgen nuevas relaciones y conductas, dentro de las relaciones tenemos que se genera empleo, nuevas áreas de estudio y facilidades a la población; con las conductas evidenciamos que se originan nuevos males hacia la misma informática y sociedad, conductas que deben ser reguladas y normadas para un mejor control y seguridad con respecto a los sistemas informáticos y la información almacenada en estos para proteger derechos en general de los usuarios de las TIC.

En el Ecuador el Derecho Informático ha presentado deficiencias graves, al no contar con legislación actualizada respecto de este tema, no es hasta el 2002 que se publicó en el Registro Oficial la Ley de Comercio Electrónico, Firmas y Mensajes de Datos misma que viene a regular los denominados: "mensajes de datos, firmas electrónicas, servicios de certificación, contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de la información además el comercio electrónico y la protección de los usuarios de estos sistemas" (Ley de Comercio Electrónico, Firmas y Mensaje de Datos, 2002, p. 1).

Esta ley en sus considerandos aclara que es necesario que se inculque la educación informática dentro de la sociedad ecuatoriana, puesto que, con la aparición de la internet, el comercio

evoluciono y ahora se puede realizar de manera tecnológica, por ende, sería necesario que las personas conozcan como opera este tipo de comercio y la tecnología en general, para que así se dé un buen desarrollo de la actividad comercial y además se agilice cualquier proceso identificado a esta ley.

De hecho, en esta Ley es que por primera vez se tipifican los delitos informáticos en el Ecuador, en una reforma de Ley que se dio el 17 de abril del 2002, en donde a través de este cuerpo normativo se incorporan reformas al Código Penal vigente en esa fecha, dicha modificación se efectuó a través del Título IV desde el articulo 57 al 64 de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos. A partir de esta reforma se consideran y sancionan delitos relacionados con el uso indebido de computadoras, redes y sistemas informáticos.

Con el pasar del tiempo el Derecho Informático empezó a tomar fuerza por lo que era necesario establecer regulaciones jurídicas más acordes al contexto tecnológico actual, es por eso que la Constitución de la República del Ecuador del 2008 siendo una constitución garantista de derechos en su Título II Derechos Capítulo II Derechos del Buen Vivir Sección 3ª Comunicación e información Artículo 16 establece:

Art. 16.- Derecho a la Comunicación. – Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre e intercultural, incluyente, diversa, participativa, en todos los ámbitos de interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social, y el acceso en igualdad de condiciones de uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación (Constitución de la República del Ecuador, 2008, p. 12).

El numeral 2, nos hace referencia a que toda la ciudadanía ecuatoriana tienen el libre acceso a las TIC, derecho fundamental que complementa el libre acceso a la comunicación y a la libertad de expresión, este acceso nos abre las puertas a un sinfín de tecnologías desde celulares,

computadoras, televisores, laptops, tablets, etc. En general dispositivos que hoy en día cualquier persona tiene en su mano o en su casa, y que además son indispensables en esta sociedad globalizada.

El siguiente numeral también nos establece que existe el derecho a la creación de medios de comunicación social, el uso de frecuencias para las estaciones de radio y televisión, además la explotación de redes inalámbricas. Derecho que se complementa con el del anterior numeral, porque ambos abren un camino infinito de posibilidades dentro del campo informático dando acceso a la creación y uso de las TIC, dando como resultado fuentes de trabajo y de estudio y por ende fuentes de ingresos a los hogares de las personas que se dedican a este campo tan sofisticado que es la informática.

Avanzando en la misma Carta Magna en su Título III Garantías Constitucionales Capítulo III Garantías Jurisdiccionales Sección 5ª Artículo 92, dispone que:

Art. 92.- Acción de hábeas data. – Toda persona por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Así mismo tendrán derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados (Constitución de la República del Ecuador, 2008, p. 37).

Esta denominada garantía jurisdiccional protege el acceso a la información y el resguardo de la misma, ya sea en físico o en un sistema informático, sirve para resguardar y garantizar que dicha información sea tratada de manera legal y no se difunda sin el permiso o consentimiento ya sea por parte de un juez o del propietario. Sirve también para estar informados con respecto a que se hace, para que la utilizan, en donde la almacenan y a donde envían la información, tanto instituciones públicas como privadas. Sin duda alguna esta garantía jurisdiccional juega

un papel fundamental dentro del Derecho Informático en el Ecuador, porque es indispensable normar el tráfico de información mediante sistemas informáticos, información delicada como lo son los datos personales, actas de propiedad de bienes entre otras.

Seguidamente tenemos la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, vigente desde el 31 de marzo de 2010 creada con la única finalidad y objeto de regular el sistema de registro públicos, la Asamblea Nacional señala que dicha Ley:

> Garantiza la seguridad jurídica, organiza, regula, sistematiza e interconecta la información, así como la eficacia y la eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías. Asegura la confidencialidad de los datos de carácter personal tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales (Asamblea Nacional del Ecuador, 2010, p. 1).

Se evidencia un avance significativo en la regulación acerca de las relaciones derivadas de la tecnología y las personas dentro del Ecuador, con la expedición de esta ley se refleja la preocupación de la legislación con respecto al avance de la tecnología y se pretende garantizar la protección de los usuarios y de su información.

El acceso libre al internet es ahora una parte esencial de la vida actual, ya que es un elemento indispensable para poder garantizar la libertad de expresión, la participación política entre otros derechos fundamentales. Este ofrece un espacio de gran valor donde las comunidades marginadas dan inicio al cambio y forjan sus identidades.

La sociedad actual podría denominarse como una sociedad tecnológica modernizada, porque cada vez es más frecuente que todo se computarice y se use bases de datos para almacenar prácticamente toda la información de las personas. Hoy en día todo está registrado en computadoras, ya que estas herramientas son capaces de almacenar cantidades exorbitantes de información, que antiguamente por su volumen era muy difícil manejarlas, ahora con un par de clics se puede tener acceso a toda la información de la historia de la humanidad recolectada hasta el día de hoy. Es por esto que el Derecho Informático toma fuerza en estos últimos años. Como manifestación del Derecho Informático a nivel mundial tenemos los derechos de cuarta generación denominados: Derechos sobre desarrollo tecnológico, las TIC y el ciberespacio.

Derechos que nos hacen mención al libre acceso a las Tecnologías de la Información y la Comunicación. Como tal, este derecho no está explícitamente en la declaración universal de los derechos humanos, pero se puede entender que se encuentra tácitamente en el artículo 19 de la misma.

> Todo individuo tiene derecho a la libre opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión (ONU, Declaración Universal de los Derechos Humanos, 1948, p. 6).

El 4 de julio de 2018 la ONU dio a conocer resoluciones sobre los derechos humanos en internet, de manera tacita se reconoció el derecho al acceso a internet. Como es de conocimiento público la información y la expresión o manifestación de ideas de las personas, necesitan de transparencia y de mecanismos de difusión que obligatoriamente, en la sociedad actual, son las nuevas y más recientes tecnologías de la información y comunicación. En la anteriormente mencionada resolución se: "Reconoce la naturaleza global y abierta de internet como fuerza motriz de la aceleración de los progresos en la consecución del desarrollo en sus diversas formas, especialmente el logro de los Objetivos de Desarrollo Sostenible" (ONU, Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluidos el derecho al desarrollo. , 2018, p. 1). En esta resolución el Consejo de Derechos Humanos se guía por la Carta de las Naciones Unidas y reafirma los derechos humanos consagrados en la Declaración Universal de Derechos Humanos y otros tratados internacionales, en este documento se acuerda una serie de resoluciones de importancia trascendental para la era actual sobre la libertad de opinión, expresión y privacidad en la era digital.

En dicha resolución, tenemos que la ONU invita a los estados a promover la educación digital y además facilitar el acceso a la información en Internet, de igual forma promover la igualdad de oportunidades en el uso de tecnologías de la información y comunicación, con atención específica a las consideraciones de género. Se alienta a los estados a adoptar medidas para garantizar la seguridad en internet, conforme a las obligaciones internacionales de derechos humanos.

Con esta resolución es evidente que a nivel internacional es una preocupación el regular aspectos fundamentales acerca de la globalización de la sociedad, de esta forma el Derecho

Informático juega un papel crucial para el desarrollo de leyes y normas que establezcan una forma segura de interactuar con la tecnología y el internet.

En el país vecino Colombia mediante el Decreto 1360, del 23 de junio de 1989, se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor, mediante este acto se refleja el comienzo que toma el derecho informático en Colombia.

Mas adelante en 1991, se agrega el derecho a la protección de datos como lo es el Habeas Data en el artículo 15 de la Constitución Política de Colombia.

Si bien en la Constitución Política de Colombia no se establece expresamente el derecho al acceso a las TICS, en la Ley 1341 del 2009 se nos establece formas para complementar algunos artículos de la Constitución y además nos da normas claras acerca de este derecho. Dicha ley tiene como finalidad determinar el marco general para la formulación de las políticas públicas que regirán el sector de las TICS, su ordenamiento general, el régimen de competencia, la protección al usuario, etc. Pero sobre todo nos adentra al derecho universal al acceso a las tecnologías de la información y la comunicación.

ARTÍCULO 2.- *Principios orientadores.* La investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Las Tecnologías de la Información y las Comunicaciones deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

Son principios orientadores de la presente ley:

11. Universalidad: el fin último de intervención del Estado en el Sector TIC es propender por el servicio universal a las Tecnologías de la Información y las Comunicaciones.

ARTÍCULO 4.- *Intervención del Estado en el sector de las Tecnologías de la Información y las Comunicaciones.* En desarrollo de los principios de Intervención contenidos en la Constitución Política, el Estado intervendrá en el sector de las Tecnologías de la Información y las Comunicaciones para lograr los siguientes fines:

2. Promover el acceso a las Tecnologías de la Información y las Comunicaciones, teniendo como fin último el servicio universal. (El Congreso de Colombia, 2009, p. 4).

Teniendo en cuenta esto podemos esclarecer que el derecho al acceso a las TICS no se encuentra como tal establecido y normado en la Constitución Política de Colombia, más sin embargo dentro de esta Ley, nos encontramos que el Estado Colombiano es el que se encargará de promover el acceso a estas tecnologías, de igual manera en esta ley se nos hace referencia que con respecto al acceso a este tipo de tecnologías, el país de Colombia se acoge a las recomendaciones de los organismos internacionales expertos en la materia, por ende se puede deducir que se reconoce el libre acceso a las TICS.

Finalmente, esta norma alude a que el acceso a las TICS es indispensable y tiene correlación con derechos como a la libertad de expresión, a la educación y a la comunicación, por lo tanto, es indispensable promover políticas públicas para poder regular el acceso y uso de las mismas.

En el vecino país Perú, recientemente se enmendó la Constitución Política en donde se añadió un párrafo al numeral cuatro del artículo dos: "El Estado promueve el uso de las tecnologías de la información y la comunicación en todo el país" (Constitución Política del Perú, 1993, p. 1).

Aquí se destaca el Derecho Informático, entrando a jugar un papel fundamental en el estado vecino, ya que estas regulaciones se vienen dando de acuerdo a la realidad del país, aunque un poco atrasadas para la actualidad, regulan y controlan las nuevas realidades de la sociedad globalizada y poco a poco establecen derechos importantes para la sociedad peruana.

En Costa Rica el Derecho Informático es: "Una disciplina jurídica que se centra en la regulación y protección de la información digital, las tecnologías de la información y la comunicación (TIC), y las actividades realizadas en el ciberespacio" (Legal Center Abogados, 2022, p. 1).

> "A un año de haber asumido el gobierno en Costa Rica, el presidente Rodrigo Chaves destacó en su informe de labores que uno de los principales logros en materia digital fue reconocer el acceso a las telecomunicaciones y las Tecnologías de la Información y Comunicaciones (TIC) como un derecho fundamental." (García, 2023, p. 1).

En este país, aún se mantiene como proyecto de ley el derecho al acceso a las TICS, sin embargo, la Corte Suprema de Justicia de Costa Rica en el año 2010, en la resolución de una disputa declaró que el acceso al internet es un derecho fundamental.

4.2. Importancia del Derecho Informático

Hoy en día, con las nuevas relaciones que aparecen por el uso del internet y en general de las TICS, el Derecho Informático comienza a tomar un papel fundamental, se origina la necesidad de normar y regular estas conductas, puesto que como es algo nuevo no se sabe aún el alcance y consecuencias que puedan tener estos comportamientos.

"El Derecho Informático va adquiriendo mayor importancia y trascendencia en los tiempos modernos, al plantear soluciones legales adecuadas a los problemas generados por el uso de la informática en sociedad sobre todo en materia de compras estatales por medios electrónicos" (Céspedes, 2000, p. 301).

Un ejemplo de esto, es la necesidad de regular el comercio electrónico, conducta que surge a partir de comprar bienes o servicios a través de medios informáticos, en general a través del internet, a este tipo de comercio también se lo define de la siguiente manera: "Se refiere a toda transacción civil, comercial o financiera, contractual o no que se efectué a través del intercambio de mensajes de datos o medios similares." (Imbaquingo Narváez et al., 2019, p. 26). El papel que toma el Derecho Informático dentro de este campo vendría dándose, en el Ecuador, con el surgimiento de la Ley de Comercio Electrónico, Firmas y Datos.

Ahora bien, al momento de relacionarse con los medios informáticos, la sociedad explora un nuevo mundo, mundo que no conoce por completo, por ende está expuesto a que le ocurran sucesos dañinos a su persona o a sus derechos, estos sucesos son el resultado de las actividades de personas que usan las tecnologías con el fin de hacer daño o sacar algún provecho de manera ilícita, estos actos son denominados delitos informáticos, por ende, surge la necesidad de que se tipifique las actividades ilegales que se realizan a través de estas tecnologías, por eso es que actualmente en la legislación penal de los países podemos encontrar al menos un tipo penal que sea denominado como delito informático.

> El Derecho Informático, como una nueva creación jurídica es de gran importancia, ya que se encarga de buscar soluciones a los retos planteados por la evolución de las aplicaciones de las computadoras electrónicas. Esta rama del Derecho está en constante seguimiento y estudio de los avances, adelantos y transformaciones tecnológicas a fin de ir planteando las medidas adecuadas que permitan una armónica convivencia social (Salazar, 2013, p. 1).

Si no se estudiara o no se aplicará el Derecho Informático las relaciones existentes entre la sociedad y la informática serían un completo caos. Así se evidencia que es de vital importancia esta rama del derecho porque controla y regula toda conducta o comportamiento que se origina de la interacción que se da entre los usuarios (personas naturales y jurídicas) y la informática.

En Ecuador se evidencia la importancia del Derecho Informático al momento de que las personas y el país comienza a globalizarse y el comercio electrónico, la educación y los delitos comienzan a darse por medio de herramientas informáticas. Esto tomo mayor fuerza durante la pandemia del COVID-19, que puso a todo el mundo en un encierro que provocó el uso obligatorio de las Tecnologías de la Información y la Comunicación para absolutamente todo: para el trabajo, para el comercio, para la información, para la educación etc.

El Acceso a las TICS también es un complemento indispensable para derechos reconocidos constitucionalmente como lo son el derecho a la libertad de expresión, a la información y comunicación, a la educación, al trabajo, ya que actualmente por medio de estas tecnologías es que se realizan y se evidencia el desarrollo de estos derechos. Es así que el Derecho Informático cumple un rol importante en lo que es la prevención de situaciones no deseadas por parte de los usuarios y en caso de que se presenten, este mismo presenta medios que facilitan la solución de los problemas causados por usar dispositivos electrónicos.

4.3. Delito

"Etimológicamente, la palabra delito proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena. En general, culpa, crimen, quebrantamiento de una ley imperativa" (Cabanellas, 2005, p. 93). Esta definición que nos da el Jurista Guillermo Cabanellas de Torres nos hace referencia a que el delito es una acción que va en contra de los establecido por la ley y que como consecuencia tiene una sanción.

En la doctrina como en los diferentes cuerpos normativos encontramos una diversidad de criterios jurídicos sobre el estudio del delito puesto que a lo largo de los años se ha dado una definición según el pensamiento de la época así hasta llegar a nuestros días, por ejemplo: "Calificación jurídica de una conducta, de acción u omisión, dolosa o culpable, determinada típicamente y castigada como tal por la ley penal" (Couture, 2006, p. 209). El jurista Eduardo Couture nos detalla de manera más descriptiva lo que es un delito, primero nos explica que es una conducta es decir una acción u omisión que surgen de un comportamiento del ser humano, que puede ser dolosa, es decir con intención, y culpable, que significa que el autor lo hace sabiendo que sus acciones pueden generar un daño, pero no tiene esa intención, sin embargo lo

hace y nos da como resultado una acción dañina, y por último este hecho tiene un castigo que se refleja en la ley penal.

El jurista Carrara nos establece que: “Delito es la infracción de la ley del Estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso” (Carrara, como se citó en Albán, 2015, pág. 102). Este concepto hace alusión a que el delito es un acto que va en contra de la ley propuesta por un Estado, es decir son acciones u omisiones que solo el hombre puede realizar y que se pueden ver y comprobar, que estan prohibidas en la ley o que son contrarias a lo que la ley establece, siendo que estos actos pueden ser reprochados a su autor, es decir que el autor tiene la capacidad de decidir si se somete a la ley o va contra ella. Y finalmente, gracias a este acontecimiento se perjudica a la sociedad. Ya que la ley que se infringió, está promulgada con el fin de una convivencia pacífica entre los habitantes del Estado.

Tenemos también la definición del tratadista Beling, que nos dice: “El delito es una acción típica, antijurídica, culpable cubierta con una sanción penal adecuada a la culpabilidad, y que llena las condiciones legales de punibilidad” (Peña y Almanza, 2010, como se citó en Ramírez, 2023, pág. 63). En síntesis, de estas nociones doctrinales, se puede concluir que los delitos son un conjunto de acciones externas del hombre, antijurídicas, tipificadas y punibles, es decir que van en contra de las leyes establecidas en la sociedad para el bienestar común y tienen como consecuencia una sanción penal que se adecua al nivel de culpabilidad de sus autores.

Con respecto a nuestra legislación, no encontramos como tal una definición de delito, pero en el artículo 18 del Código Orgánico Integral Penal se establece lo que es la infracción penal así: “Art. 18.- Infracción Penal. - Es la conducta típica, antijurídica y culpable cuya sanción se encuentra prevista en este Código” (Código Orgánico Integral Penal, 2014, p. 14). En el siguiente artículo nos refiere que “Las infracciones se clasifican en delitos y contravenciones” (Código Orgánico Integral Penal, 2014, p. 14). De esta manera se puede deducir que delito es una infracción penal típica, antijurídica, culpable y que como consecuencia existe una sanción establecida dentro del marco legal.

De todas estas definiciones y nociones doctrinales, se puede afirmar que los delitos son un conjunto de conductas, ya sean acciones u omisiones propias del hombre que son antijurídicas, típicas, culpables y punibles, o sea que van en contra de las leyes establecidas en la sociedad para el bienestar común y como consecuencia se les atribuye una sanción penal como lo es una pena privativa de libertad, multa etc.

4.4. Estructura del delito

Las definiciones actuales determinan aspectos fundamentales para identificar lo que es un delito, casi todas estas nociones están de acuerdo en los elementos que un delito debe tener para ser considerado como tal, estos son: acto, tipicidad, antijuridicidad y culpabilidad. Si se dan estos presupuestos, la acción que se está calificando se considera como sancionable.

De esta forma no basta con que la ley exprese que existe un delito, sino que hay que determinar que estos elementos consten para que la legislación penal pueda calificarlos como delitos y de esta forma castigarlos.

4.5. El Acto

"Manifestación de voluntad o de fuerza. Hecho o acción de lo acorde con la voluntad humana" (Ossorio, 2008, p. 36). Partiendo de este concepto podemos alegar que el acto es una acción que nace de la voluntad del hombre, es decir que lo realiza queriendo. Vinculándolo al delito, el acto es la manifestación externa de la voluntad del hombre de manera dañina hacia un bien jurídico protegido por la Ley.

> El primer elemento del delito es el acto. Con esto se quiere establecer que el acto es el elemento de hecho, inicial y básico del delito. Para que haya delito entonces, lo primero será determinar la corporeidad material y tangible de este ente jurídico, para que luego se verifique su adecuación a la descripción hecha por la ley (tipicidad) y se realicen los juicios de valor, objetivo (antijuridicidad) y subjetivo (culpabilidad), que constituyen los otros elementos del delito. Por esta razón este primer elemento es un sustantivo, acto, al cual se agregan los otros tres, como adjetivos que lo califican: acto típico, antijurídico y culpable (Albán, 2018, p. 131).

El maestro Albán nos explica que para que se conforme un delito primeramente se necesita de un acto o acción, misma que vendría a ser el realizar o ejercer algo y una vez que se confirmó la existencia de este, se puede agregarlo a la ley, no sin antes comprobar si consta con las características adecuadas que vendrían siendo la antijuridicidad y la culpabilidad. En relación al concepto de acto el Dr. Albán nos explica que: "Acto es la conducta humana guiada por la voluntad. Hace falta, pues, un contenido básico de voluntad, entendido simplemente como el dominio que el ser humano ejerce sobre su actividad (o sobre su inactividad, en los delitos de omisión)" (Albán, 2018, p. 131).

El acto es la conducta voluntaria, la persona debe exteriorizar su voluntad, debe realizar lo que desea para formalizar el acto o la omisión, puesto que, si solo lo desea o lo piensa, pero no lo ejecuta, no se manifiesta la voluntad, no se da un acto como tal, por lo tanto, no existe un delito. No podría existir un delito sino se manifiesta una conducta, esta conducta debe ser de importancia para la sociedad.

Por su parte los autores Muñoz y García nos refieren:

> Se llama acción a todo comportamiento dependiente de la voluntad humana. Sólo el acto voluntario puede ser penalmente relevante y la voluntad implica siempre una finalidad. No se concibe un acto de la voluntad que no vaya dirigido a algún fin u objetivo determinado (Muñoz y García, 2015, como se citó en Girón, 2021, pág. 21).

Analizando estas nociones nos damos cuenta que el acto vendría a ser una exteriorización de la voluntad o pensamientos del hombre, es decir que realice una acción o una omisión, y que la finalidad de estos sea de importancia para el ámbito penal.

Desde la perspectiva legal, en nuestra legislación dentro del Código Orgánico Integral Penal, en el artículo 22 se nos alega que los delitos son acciones u omisiones, dándonos a entender que si no hay acción u omisión no hay delito. El legislador nos dice: "Art. 22.- Conductas penalmente relevantes. - Son penalmente relevantes las acciones u omisiones que ponen en peligro o producen resultados lesivos, descriptibles y demostrables" (Código Orgánico Integral Penal, 2014, p. 14). Este artículo nos exige una relación de causa efecto entre el acto y el resultado que nos deje este, en este caso el poner en peligro bienes jurídicos o dañarlos, pero estos actos se tienen que poder describir y demostrar.

4.5.1. Modalidades del Acto

El acto se nos presenta de dos formas: la acción y la omisión. De esta forma se puede deducir que existen dos tipos de delitos, los delitos de acción y delitos de omisión.

Guillermo Cabanellas de Torres acerca de acción nos explica que: "Del latín agere, hacer, obrar (…) Efecto o resultado de hacer" (Cabanellas, 2005, p. 9). La acción vendría siendo el realizar o cometer la conducta o el delito, ejecutar físicamente lo que se piensa dando un resultado de daño.

Siguiendo las enseñanzas de la doctrina el jurista Ernesto Albán se refiere a la acción de la siguiente manera:

> Es la modalidad característica de la gran mayoría de delitos. Se manifiesta como un movimiento humano externo, como un hacer perceptible sensorialmente, que causa el resultado dañoso. Se puede decir que al cometerse estos delitos se incumple una norma prohibitiva, una obligación de no hacer (Albán, 2018, p. 133).

En resumidas cuentas, la acción viene del ser humano al realizar un movimiento externo, en el caso de los delitos, sería por ejemplo una persona que revela información de manera ilegal violando el secreto o la intimidad de las personas, para esto el hombre tiene que realizar varias acciones dentro de un sistema informático, ya que la información no se va a revelar solo con pensarlo. Esta acción es demostrable y se puede percibir ya que causa un daño externo que todos pueden notarlo. Al realizar esta acción, se comete un delito establecido dentro del marco legal, por ende, tiene como resultado una sanción penal.

Siguiendo con la omisión en el diccionario de ciencias jurídicas políticas y sociales del maestro Manuel Ossorio se la define así: "Abstención de actuar" (Ossorio, 2008, p. 655). Con esta definición podemos alegar que la omisión vendría siendo el no hacer algo, el no actuar o el no realizar una acción en sí. Dentro de la doctrina podemos encontrar que existe un convenio tácito entre los diversos autores del derecho penal al definir o explicar lo que es la omisión, así por ejemplo tenemos las palabras del Dr. Ernesto Albán:

> La omisión, en cambio, se manifiesta como un voluntario no hacer algo, que debía haberse hecho y que se exterioriza (pues necesariamente en todo delito debe haber exteriorización), con un resultado lesionador de un bien jurídico, que no debía haberse producido si se actuaba. En estos delitos se incumple una norma mandataria que imponía una obligación de hacer (Albán, 2018, p. 133).

Afirmamos que la omisión es la voluntad humana de no llevar a cabo una acción realmente necesaria y que al momento de efectuarse se la puede percibir sensorialmente porque resulta que daña a un derecho protegido, este tipo de delitos son porque la persona que los comete de una manera pasiva omite la realización de un mandato legal

En nuestra legislación podemos encontrar que se encuentran establecidos estos dos tipos de delitos, ya que, nuestro Código Orgánico Integral Penal en el artículo 23 encontramos: "Art. 23. - Modalidades de la conducta. – La conducta punible puede tener como modalidades la acción y la omisión. No impedir un acontecimiento, cuando se tiene la obligación jurídica de impedirlo, equivale a ocasionarlo" (Código Orgánico Integral Penal, 2014, p. 14). Se evidencia que en el Ecuador existen acercamientos a las nociones doctrinales acerca del delito, un caso

concreto es este, en donde se establece que existen dos tipos de delitos, los de acción y omisión, dándonos un marco legal claro y contundente al momento del estudio de conductas de relevancia penal, garantizando de esta manera el libre goce de los derechos de la ciudadanía.

4.5.1.1. Causas de exclusión de la conducta

"Si el acto, en sentido penal, es una conducta humana guiada por la voluntad, los movimientos corporales sin contenido de voluntad, aunque causen daños, no pueden ser considerados como actos" (Albán, 2018, p. 138).

Dentro del ámbito penal existen causas que excluyen la conducta, es decir circunstancias en las que las acciones no son realizadas por la voluntad de la persona, sino que las realizan sin ser premeditadas ni planeadas, estos son casos particulares que se deben analizar al momento en el que se está determinando si existe o no el delito, ya que si no existe la voluntad estos hechos no vendrían siendo delitos, pues un acontecimiento sin voluntariedad no es considerado como un acto, por lo tanto, se pierde el elemento esencial del delito. Con esto bastaría para dejar de buscar los siguientes elementos constitutivos del delito, estas causas varían según los doctrinarios, pero entre las más comunes encontramos las siguientes: fuerza física irresistible, el sueño natural, el sonambulismo y los movimientos reflejos.

Con respecto a la fuerza física irresistible vendríamos diciendo que es una fuerza externa a la persona que se es incapaz de resistir, al respecto Zaffaroni nos dice: "Los que tienen lugar porque la persona es incapaz de voluntad en el momento del hecho (involuntariedad) o porque una fuerza le impide actuar conforme su voluntad" (Zaffaroni, 2009, como se citó en Montero, 2023, pág 65). Como ejemplo de este enunciado podemos decir que dos personas están en lo alto de una montaña y el viento es fuerte y empuja a una persona sobre la otra, la cual cae y muere. La persona no se pudo resistir al viento (fuerza física irresistible) y no fue voluntad de ella matar a su compañero.

Dentro del Ecuador, en el Código Orgánico Integral Penal encontramos a la fuerza física irresistible como una causa de exclusión de la conducta, y este nos refiere que "no son penalmente relevantes los resultados dañosos o peligrosos resultantes de fuerza física irresistible…" (Código Orgánico Integral Penal, 2014, p. 14). Entonces este artículo nos explica que no existe pena si esta causa se ejecuta dentro de la conducta.

Continuando con el sueño natural propuesto por la doctrina, esta se refiere a un estado en donde la persona se encuentra en reposo: "Cuando usted duerme está inconsciente, pero las funciones

de su cerebro y cuerpo siguen activas" (MedlinePlus, 2024, p. 1). Refiriéndonos a esta explicación podemos deducir que cuando una persona duerme no tiene el control de su voluntad, puesto que entra en un estado donde no tiene conciencia de lo que hace, de hecho, no realiza nada más que movimientos involuntarios.

El jurista Manuel Ossorio con respecto a este tema nos explica:

> De otro lado es excusante de responsabilidad, por falta de conciencia y voluntad, sea por movimientos durante el mismo, como la madre que asfixia al hijito con el que duerme en la cama o, con otra clase de movimiento, en acto de sonambulismo (Ossorio, 2008, p. 921).

Como ya sabemos en el ámbito del derecho penal, para que pueda existir un acto como tal debe constar la voluntad y conciencia de la persona, la carencia de estos elementos eximen de responsabilidad jurídica al actor, un ejemplo de esto es el sueño, un estado en donde la persona reduce la actividad consciente del cerebro, es así que la misma no tiene control voluntario de sus acciones, Ossorio nos pone como ejemplo a la madre que asfixia a su hijo por un movimiento que se produce durante el sueño, en este caso es evidente que la madre no tuvo la voluntad de matar a su hijo, sino más bien fue un movimiento inconsciente que se produjo cuando estaba en un estado profundo de sueño, sin darse cuenta siquiera que está asfixiando a su hijo, por ende se exime de toda responsabilidad a la autora.

En el Código Orgánico Integral Penal no está descrito el sueño como tal, sin embargo, el mismo nos refiere: "estados de plena inconciencia, debidamente comprobados" (Código Orgánico Integral Penal, 2014, p. 14). Aquí se aplicaría este caso en concreto.

El sonambulismo como tal es un estado en donde la persona que duerme realiza actos en un estado de plena inconciencia y que cuando despierta piensa que simplemente fueron sueños. En el diccionario del jurista Ossorio encontramos definido este término de la siguiente manera:

> Estado de sonámbulo, o sea aquel en que se encuentra la persona que por afección natural o por sugestión padece sueño anormal, durante el que tiene cierta aptitud para ejecutar algunas funciones correspondientes a la vida de relación exterior, como las de levantarse, andar y hablar (Ossorio, 2008, p. 910).

Este estado exime totalmente de acción al autor de alguna conducta que lesione o dañe algún bien jurídico penalmente protegido, porque de igual manera que en el sueño natural, esta

persona realiza el hecho sin voluntad, elemento indispensable de la conducta del delito, además, este se encuentra en un estado de inconciencia, es decir, no sabe lo que está haciendo.

Adentrándonos a la legislación ecuatoriana, de igual manera que en el sueño natural, no se encuentra establecido dentro del Código Orgánico Integral Penal, pero también se aplica la misma referencia del artículo 24 concerniente a los estados de plena inconciencia, que puedan ser comprobados.

Finalmente, con los movimientos reflejos, que según la doctrina son movimientos automáticos carentes de voluntad de la persona, son una causa que excluye conducta y que por ende resulta la no existencia del delito. El doctor Ernesto Albán nos explica que:

> Estos son movimientos automáticos que se producen como reacción corporal orgánica ante estímulos externos o internos: el movimiento de la mano como acto defensivo, el cerrar los ojos, un estornudo, la salivación, y otros similares. Estos movimientos son generalmente intempestivos y sobre ellos la voluntad no ejerce control, salvo casos excepcionales en que la persona puede hacerlo en cierto vencimiento (Albán, 2018, p. 141).

Con esta explicación del doctor Albán solo surge una cuestión, ¿hay voluntad en este tipo de movimientos? Claro que no, puesto que son movimientos que surgen como respuesta de un estímulo externo o interno como un mecanismo de defensa propios del cuerpo en donde la voluntad no juega ningún papel.

En el Ecuador, nuevamente nos adentramos al artículo 24 del Código Orgánico Integral Penal en donde si encontramos descritos los movimientos reflejos como una causa de exclusión de la conducta.

4.6. Tipicidad

La tipicidad como tal es adecuar a la ley penal el hecho analizado, no sin antes pasar por un filtro por el cual la conducta es descrita por el legislador. Respecto a este término, nos explica el jurista Guillermo Cabanellas que:

> Concepto muy discutido en el Derecho Penal moderno, entre otras razones porque guarda relación con el Derecho Penal liberal, del cual es garantía, que se vincula con el principio del *nullum crimen sine praevia lege.* Jiménez de Asúa, refiriéndose a Beling, creador de la teoría, dice que la vida diaria nos presenta una serie de hechos contrarios a la norma y que por dañar la convivencia social se sancionan con una pena, estando

> definidos por el código o las leyes, para poder castigarlos. “Esa descripción legal, desprovista de carácter valorativo, es lo que constituye la tipicidad. Por tanto, el tipo legal es la abstracción concreta que ha trazado el legislador, descartando los detalles innecesarios para la definición del hecho que se cataloga en la ley como delito”. Añade que en la tipicidad no hay “tipos de hechos”, sino solamente “tipos legales”, porque se trata de la conducta del hombre que se subsume en el tipo legal (Cabanellas, 2005, p. 461).

Como se puede apreciar este elemento del delito es algo nuevo que se discute en el Derecho Penal moderno, porque se relaciona directamente con el principio de legalidad no hay delito ni pena sin ley. Entonces la tipicidad viene siendo la descripción del delito dentro de la norma penal de un estado. En la sociedad se evidencia un sinfín de hechos que violan las leyes y que además van en contra de la convivencia entre la sociedad y como consecuencia reciben un castigo denominado pena. Con respecto a lo que nos refiere Jiménez de Asúa sobre la tipicidad se puede decir que la tipicidad es una descripción que se manifiesta de manera neutral y objetiva, sin emitir juicios de valor u opiniones subjetivas sobre la conducta descrita. Por ende, el tipo legal se refiere a la descripción normativa de una conducta, en la cual el legislador excluye detalles irrelevantes y en su lugar destaca las características esenciales que definen a un delito, evitando profundizar en aspectos innecesarios.

Podemos concluir que la tipicidad es el establecer la conducta humana ya sea de acción o de omisión, de manera descriptiva en la normativa legal vigente, garantizando así que este delito pueda ser investigado y juzgado dentro de la sociedad, garantizando así el libre ejercicio de los derechos de la ciudadanía. También se puede decir que aparte de ser un elemento del delito, podría ser un principio del derecho penal, porque sin esta es obvio que no se podría sancionar y juzgar un delito que no está establecido como tal.

Por otro lado, se nos menciona que la tipicidad es:

> La característica o cualidad que tiene una conducta (acción u omisión) de encuadrar, subsumir o adecuarse a un tipo penal.
>
> Ahora bien, tipificar es la acción de encuadrar la conducta en un tipo penal. Este acto de tipificar lo realiza el fiscal, la defensa, la policía o el estudiante; sin embargo, cuando lo hace el juez se le denomina tipificación judicial (Girón, 2021, p. 65).

Dentro del Ecuador, la tipicidad está establecida dentro del Código Orgánico Integral Penal en el artículo 25 y nos menciona que: "Tipicidad. – Los tipos penales describen los elementos de las conductas penalmente relevantes." (Código Orgánico Integral Penal, 2014, p. 15).

De esta manera podemos observar que nuestra legislación ha adoptado la doctrina del derecho penal en relación con la tipicidad, definiéndola de manera clara y concisa, sin ambigüedades ni rodeos innecesarios.

4.7. Antijuridicidad

Resumidamente la antijuridicidad es el conjunto de conductas que están en contra de lo establecido dentro de una normativa legal para el bienestar común. Los doctrinarios nos dan como concepto lo siguiente: "Elemento esencial del delito, cuya fórmula es el valor que se concede al fin perseguido por la acción criminal en contradicción con aquel otro garantizado por el Derecho" (Cabanellas, 2005, p. 32). La antijuridicidad es importante dentro del derecho penal, porque es la cualidad que tiene una conducta de ser contraria al ordenamiento jurídico, es decir, de infringir o violar una norma legal que protege bienes jurídicos indispensables para las personas, sin este elemento el acto no puede ser tomado como un delito.

Por otro lado, tenemos la definición del doctor Albán, que nos indica: "Que una conducta o un acto sean antijurídicos significa, exactamente, que se trata de una conducta o un acto contrarios al orden jurídico" (Albán, 2018, p. 163). Bien, aquí se evidencia que los doctrinarios han llegado a un tratado tácito en donde el concepto de antijuridicidad es el mismo, que el acto o la conducta del hombre viola o van en contra de un bien jurídico protegido por un estado, por ejemplo tenemos una persona que roba información de otra y la revela sin ningún permiso de la persona afectada, en este ejemplo el bien jurídico afectado es el derecho a la intimidad personal y familiar, derecho que se reconoce en la Constitución de la República del Ecuador en el artículo 66 numeral 20: "El derecho a la intimidad personal y familiar" (Constitución de la República del Ecuador, 2008, p. 26). Se puede corroborar que esta acción viola y afecta un derecho establecido dentro del marco legal ecuatoriano, no sin antes que esta conducta se encuentre tipificada dentro de la ley penal.

Continuando con el estudio de la antijuridicidad el doctrinario José Girón nos afirma: "una acción u omisión es antijuridica cuando se encuadra en un tipo penal (acción típica), y no concurran causas de justificación (legítima defensa, estado de necesidad y legítimo ejercicio de un derecho)" (Girón, 2021, p. 103), desde este punto de vista, entendemos que existen causas de exclusión de la antijuridicidad también denominadas causas de justificación. El doctrinario

nos adentra a un estudio más profundo de este elemento del delito, en donde nos refiere que, si existen estas causas, la antijuridicidad vendría a ser nula.

Desde el punto de vista legal, la legislación ecuatoriana en el Código Orgánico Integral Penal con respecto a la antijuridicidad, el legislador nos establece lo siguiente: "Art. 29. – Antijuridicidad. – Para que la conducta penalmente relevante sea antijurídica deberá amenazar o lesionar, sin justa causa, un bien jurídico protegido por este Código" (Código Orgánico Integral Penal, 2014, p. 13).

Analizando lo que el legislador nos explica, encontramos que existen elementos indispensables sobre la antijuridicidad. En primer lugar, se nos afirma que debe existir una conducta humana, la cual será objeto de estudio para comprobar si es antijurídica o no.

Esta conducta puede ser antijurídica de dos formas posibles, cuando amenace un bien jurídico protegido, como por ejemplo el acceso no consentido a un sistema informático, telemático o de telecomunicaciones y cuando se lesionan derechos, como modelo de esto tenemos la violación a la intimidad, aquí se verifica que un resultado, que sería revelar información de una persona, violando el derecho a la intimidad personal o familiar.

4.7.1. Causas de exclusión de la Antijuridicidad

Para poder armar un delito como tal se necesita de una conducta humana, ya sea acción u omisión, misma que debe incluirse en uno de los tipos penales regulados dentro de la legislación y que debe ser antijurídica en la que no se incurra a una causa de exclusión de la misma, entonces se puede decir que estas causas de exclusión son el elemento negativo de la antijuridicidad. Estas causas han sido materia de estudio desde tiempos antiguos y la doctrina nos dice que: "son causas que transforman un acto o conducta típica en jurídica, por ser justa y no injusta, excluyendo así la antijuridicidad o tercera categoría dogmática del delito, por tanto, se detiene el camino hacia la punibilidad" (Montero, 2023, p. 69). Analizando esto podemos decir que las causas de exclusión de la antijuridicidad son circunstancias que hacen que un acto que normalmente sería considerado delictivo no sea considerado de esta manera debido a la justificación de la conducta. Estas causas justifican la acción delictiva, transformándola en una conducta lícita. Entonces el acto, ya siendo típico, no es antijurídico porque dentro de todo el contexto existe una razón legal que lo justifica. Siendo así que al excluir la antijuridicidad se detiene por completo el proceso para considerar a esta conducta como merecedora de una pena.

Ahora bien, la doctrina ha estudiado de manera detallada estas causas y frecuentemente son cuatro, mismas que son reconocidas en el contexto legal ecuatoriano dentro del Código Orgánico Integral Penal en el artículo 30 que establece:

No existe infracción penal cuando la conducta típica se encuentra justificada por estado de necesidad o legítima defensa. Tampoco existe infracción penal cuando se actúa en cumplimiento de una orden legitima y expresa de autoridad competente o de un deber legal, debidamente comprobados (Código Orgánico Integral Penal, 2014, p. 16).

Dentro del texto legal se comprueba lo que la doctrina promueve respecto de las causas de justificación, mismas que son: estado de necesidad; legítima defensa; y cumplimiento de una orden legítima y expresa de autoridad competente o de un deber legal.

4.7.1.1. Estado de necesidad

Esta causa es una de las tratadas desde épocas antiguas e incluida en varias legislaciones, un concepto breve vendría siendo el siguiente: "situación de peligro para un bien jurídico que solo puede salvarse mediante la lesión de otro bien jurídico" (Albán, 2018, p. 173), el estado de necesidad es una causa de exclusión de la antijuridicidad que se aplica cuando una persona que se encuentra en una situación de peligro inminente para un bien jurídico como podría ser la vida, la integridad física, la propiedad etc. Y solo puede evitar ese peligro dañando otro bien jurídico de menor o igual valor.

El estado de necesidad justifica la lesión del bien jurídico a una persona cuando el derecho de otra está en riesgo de sufrir un daño inminente por parte de la primera, cuando no hay otra alternativa razonable para evitar el daño y cuando el daño que se cause debe ser menor o igual al daño que se evita, no es justificable causar un daño mayor para evitar uno menor. Un ejemplo de esto puede ser el aborto terapéutico, este tipo de intervenciones medicas es cuando una persona, mujer embarazada en este caso, no puede continuar con su embarazo porque pone en riesgo su vida y se le debe practicar un aborto de emergencia, esta acción es un estado de necesidad ya que un bien jurídico está en peligro, en este caso la vida de la mujer, y no hay otra forma más que producir el aborto lesionando la vida del feto para salvar a la señora.

Al darse esta circunstancia se excluye totalmente la antijuridicidad, la acción es típica pero no antijuridica, por ende, no se configura el delito.

4.7.1.2. Legítima defensa

Esta causa de exclusión de la antijuridicidad se da cuando la persona ejerce una acción para defenderse o defender a un tercero de un ataque de otra persona. Esta causa es la más antigua y conocida.

"El ser humano por instinto repele cualquier ataque que se produzca en contra de su integridad o de sus derechos, ello ha ocurrido desde siempre como especie" (Montero, 2023, p. 70).

Partiendo de lo que nos explica el doctrinario Juan Montero podemos deducir que es un instinto natural del hombre el poderse defender de algún ataque, esto como mecanismo de defensa, ahora bien, el derecho ha recogido esta conducta y la ha integrado como una causa de justificación al momento de llegar a comprobar la antijuridicidad de una acción.

De igual manera el doctrinario nos indica que: "con legítima defensa se repele legalmente un ataque ilegal" (Montero, 2023, p. 70).

Partiendo de este análisis podemos poner como ejemplo una persona que viene a robar a otra con un arma blanca y lo amenaza de muerte si no se somete y se deja robar, la otra persona por defender su vida y su propiedad privada le quita el cuchillo al delincuente y lo apuñala causándole la muerte, esto encaja de manera precisa en la legitima defensa.

Por su lado el jurista Ernesto Albán nos explica un concepto de legítima defensa: "rechazo de una agresión actual, ilegítima y no provocada, mediante un acto de defensa, que causa un daño al agresor" (Albán, 2018, p. 165), nos encontramos que los doctrinarios nos explican la legitima defensa de la misma forma, llegando a un acuerdo tácito entre ellos para fundamentar y explicar esta causa de justificación.

La legítima defensa es una causa de justificación de la antijuridicidad que se aplica cuando una conducta típica se lleva a cabo para proteger un bien jurídico frente a una agresión ilegitima. En otras palabras, se trata de una acción que, aunque normalmente sería considerada como una violación a la ley, se justifica si se realiza en defensa de uno mismo o de otro frente a una amenaza inminente y directa.

Cuando nos adentramos a la legislación ecuatoriana, encontramos específicamente los requisitos para concurrir en legítima defensa: "Existe legítima defensa cuando la persona actúa en defensa de cualquier derecho, propio o ajeno, siempre y cuando concurran a los siguientes requisitos:

1. Agresión actual e ilegítima.
2. Necesidad racional de la defensa.
3. Falta de provocación suficiente por parte de quien actúa en defensa del derecho" (Código Orgánico Integral Penal, 2014, p. 17).

Con estas causales se delimita la expansión de la legitima defensa, precisando hasta donde se puede acudir a esta causa de justificación. Dentro del primer requisito podemos deducir que la amenaza o ataque debe de ser inminente, es decir, debe estar ocurriendo en ese momento o estar a punto de ocurrir. No se considera legítima defensa si la agresión ya ha pasado o si es una amenaza futura y no inminente. También la agresión debe ser injustificada e ilegítima, es decir, debe ser un ataque que no tiene derecho a ocurrir.

Con respecto al segundo numeral, se deduce, que la defensa debe ser adecuada y necesaria para repeler el ataque. Esto significa que la persona que actúa en defensa propia debe utilizar el medio o la fuerza necesaria para evitar la agresión. Como ejemplo de esto podemos aducir que una persona A viene contra otra persona B con las intenciones de asesinarlo con arma blanca, la persona B en el afán de salvarse necesita de defensa y lastima la integridad física de su agresor, aquí se aplica este numeral, verificando que realmente de manera racional se necesitó de defensa propia, puesto que no había más al alcance para eludir este ataque.

Y en el numeral tercero tenemos que la persona que actúa en defensa no debe haber provocado la agresión de manera significativa. Esto significa que no se puede invocar la legitima defensa si uno mismo ha provocado deliberadamente a la otra persona para que actúe agresivamente. La provocación puede ser de diferentes tipos, como insultos o provocaciones físicas, que hacen que la defensa no sea considerada legitima si es resultado de una provocación injustificada por parte de quien se defiende.

En resumen, para que se reconozca la legitima defensa, se deben cumplir estos requisitos: la agresión debe ser actual e ilegítima, la defensa debe ser necesaria y proporcional a la amenaza, y la persona que se defiende no debe haber provocado el ataque. Si estos criterios cumplen, la acción defensiva puede ser justificada legalmente.

4.7.1.3. Cumplimiento de una orden legítima y expresa de autoridad competente o de un deber legal

Estas son unas de las causas de justificación aceptadas por la doctrina, pero como es evidente si se comete una acción que se encuentra ordenada o permitida en la ley, no debe estar

sancionada por la misma. Estas causas están más enfocadas en los servidores públicos de la policía y de las fuerzas armadas, en el Ecuador dentro del artículo 30.1 encontramos la explicación del cumplimiento del deber legal de los servidores de la Policía Nacional, Fuerzas Armadas y del Cuerpo de Seguridad y Vigilancia Penitenciaria, en donde nos explican que estos al momento de cumplir su deber mientras protejan algún derecho propio o ajeno y causan algún daño o muerte a otra persona cumplen con esta condición, no sin antes verificar el cumplimiento de algunos requisitos como por ejemplo:

"1. Que se realice en actos de servicio o como consecuencia del mismo;

2. Que, para el cumplimiento de su misión constitucional o legal, dentro de su procedimiento profesional, cumpla los principios para el uso legítimo de la fuerza, establecidos en la ley de la materia; y,

3. Que exista amenaza o peligro inminente de muerte o lesiones graves, para sí o para terceros, en los casos que se recurra al arma de fuego con munición letal" (Código Orgánico Integral Penal, 2014, p. 16).

Una vez verificado que estos requisitos se cumplan por parte de los organismos de la policía o de las fuerzas armas y guías penitenciarios dentro del país nos encontramos con una causa de exclusión de la antijuridicidad por ende no se seguiría con el estudio de la última categoría del delito.

4.8. Culpabilidad

Luego de que se verificó que el acto en cuestión es típico y antijurídico se procede con el estudio del último elemento para determinar si nos encontramos frente a un delito o no y este se denomina culpabilidad. Como concepto de esto el jurista Soler nos refiere que la culpabilidad "señala el límite de lo que puede ser imputado al sujeto como su obra, y además de la forma de esa imputación" (S. Soler, como se citó en Casado, 2008, pág 107). Para entender este concepto debemos partir desde la imputabilidad, esto se refiere a la atribución de un hecho delictivo a una persona, considerando que esta ha actuado con conciencia y voluntad. Se establece entonces que una persona solo puede ser considerada culpable de aquello que sea consecuencia directa de su conducta voluntaria y de forma consciente. En resumen, el límite de lo que puede ser imputado al sujeto como su acto rescata la necesidad de una conexión causal directa entre la conducta de una persona y el resultado delictivo para establecer su culpabilidad en derecho penal.

Ahora, tratando de definir a la culpabilidad José Gustavo Girón nos enseña lo siguiente:

> La culpabilidad puede definirse como un juicio de reproche, siempre y cuando el sujeto tenga capacidad para motivarse o determinarse de acuerdo con la comprensión de sus acciones, que además tenga conocimiento de la antijuridicidad de la conducta realizada, y que al sujeto le era exigible obrar de otro modo, y no cómo lo hizo. Cumpliendo estas circunstancias, la persona es culpable, penalmente responsable y como consecuencia del delito, se podrá imponer una pena (Girón, 2021, p. 131).

La culpabilidad según lo que nos explica Girón, implica un juicio moral y jurídico que se realiza sobre la conducta de una persona. Implica evaluar si el individuo actuó de manera consciente y voluntaria, siendo capaz de comprender la naturaleza de sus acciones y de orientar su conducta de acuerdo con ese entendimiento.

Para que una persona sea considerada culpable, debe tener la capacidad psicológica y cognitiva de motivarse o determinarse a realizar la conducta delictiva. Esto implica que no haya sido coaccionado, inducido por error invencible o ser incapaz de comprender la naturaleza y consecuencia de sus actos.

Esta persona debe de ser consciente de que sus acciones son contrarias a la ley (antijurídica). Es decir, debe tener el conocimiento y entendimiento de que lo que está realizando está prohibido por el ordenamiento jurídico.

El autor al referirse a la exigibilidad de obrar de otro modo, se refiere al hecho de que la ley determina el actuar correcto para la sociedad y sin embargo la persona comete actos contrarios al orden legal.

En conjunto, estas características definen a la culpabilidad como un criterio moral y legal para determinar la responsabilidad penal de una persona. Girón sugiere que una persona es culpable cuando, actuando con pleno conocimiento de la antijuridicidad de sus actos y teniendo la capacidad de proceder de manera distinta, decide realizar una conducta que violenta la ley. Esta comprensión subraya la importancia de la intención, la conciencia y la capacidad de elección como fundamentos para imputar responsabilidad penal a un individuo.

Dentro de la legislación ecuatoriana encontramos a la culpabilidad en el artículo 34 del Código Orgánico Integral Penal y nos indica que: “para que una persona sea considerada responsable penalmente deberá ser imputable y actuar con conocimiento de la antijuridicidad de su conducta” (Código Orgánico Integral Penal, 2014, p. 17). Bien al analizar esta explicación de

la norma penal nos damos cuenta que el legislador recoge las características de la doctrina y las plasma en el cuerpo normativo penal, dándonos a entender que la culpabilidad es que el individuo que actúa debe ser capaz de ser juzgado, es decir que no exista ninguna causa de justificación que lo excluya de culpabilidad, la persona debe estar consciente de que sus acciones son contrarias a la ley y aun así actúa de igual forma, de ser así, se le impondrá una pena legal.

Resumidamente la culpabilidad es el juicio de reproche que se le debe realizar al individuo autor de un supuesto delito, determinando si este actúa de manera consciente y comprendiendo que sus acciones son antijuridicas, declarándolo imputable y por lo tanto merecedor de una pena.

En sentido contrario, aunque una conducta pueda ser considerada típica y antijurídica, existen circunstancias en las cuales la persona no puede ser culpable penalmente. Esto incluye casos donde el individuo carece de la capacidad de comprensión de su propia conducta (como en el caso de los inimputables), o cuando la persona desconoce el contenido específico de la normativa (error de prohibición). Además, si no es exigible que el sujeto actúe de manera distinta dadas las circunstancias particulares, los objetivos de la pena no se cumplirían efectivamente en el condenado.

4.8.1. Causas de inculpabilidad

Ahora bien, al momento de verificar la culpabilidad de una conducta del hombre se debe también comprobar si esta conducta concurre en alguna causa de exclusión de la culpabilidad o también llamadas causas de inculpabilidad.

Como ya se sabe, para recaer en la culpabilidad el sujeto activo debe ser imputable, la imputabilidad podría considerarse como la capacidad que tiene la persona para comprender la desaprobación por parte del orden legal, y de igual manera, esta persona dirige su accionar de acuerdo a esta comprensión de ilegalidad. Pues bien, las causas de inculpabilidad son todo lo contrario, según la doctrina y la legislación del Ecuador son las siguientes: error de prohibición invencible y trastorno mental, igual que las causas de las anteriores categorías dogmáticas, estas se deben comprobar para que se puedan configurar.

El error de prohibición según la doctrina: “Es el elemento negativo del conocimiento de la antijuridicidad, denominado desconocimiento de la antijuridicidad, consiste en desconocer la prohibición contenida en la norma penal” (Girón, 2021, p. 145). En definitiva, un individuo

solo será culpable si conoce que el hecho que va a perpetrar vulnera el orden jurídico. Entonces, si existe un error de prohibición invencible no vendría a efectuarse la culpabilidad. El error de prohibición invencible se refiere a que la persona realmente no tenía la posibilidad de conocer la ilegalidad de su conducta. Existe también esta causal si el sujeto activo actúa pensando que su cometido está amparado en una causa de justificación que no existen o en una causa que no esté establecida en la norma legal.

Dentro del marco legal ecuatoriano, en el artículo 35.1 del Código Orgánico Integral Penal se nos establece el error de prohibición de la siguiente manera:

> Existe error de prohibición cuando la persona, por error o ignorancia invencible, no puede prever la ilicitud de la conducta.
>
> Si el error es invencible no hay responsabilidad penal.
>
> Si el error es vencible se aplica la pena mínima prevista para la infracción, reducida en un tercio (Código Orgánico Integral Penal, 2014, p. 18).

Dentro de este artículo, se establece un error de prohibición con referencia a lo que los doctrinarios nos han establecido. Al referirse que el error es invencible, se nos refiere a que la persona no tenía ninguna alternativa para conocer la ilicitud de su conducta. Esto se determinará según las cuestiones culturales, la educación, nacionalidad e incluso la naturaleza del delito cometido.

Si el actor con algún esfuerzo podría conocer la antijuridicidad de su conducta y realiza el acto pues se aplica la mínima pena establecida, pero reducida en un tercio.

Por otra parte, el trastorno mental, perturbación mental entre otras denominaciones, está tomada en cuenta como una situación de inimputabilidad, según la Organización Mundial de la Salud: "Un trastorno mental se caracteriza por una alteración clínicamente significativa de la cognición, la regulación de las emociones o el comportamiento de un individuo" (OMS, 2022, p. 1).

En este concepto la OMS nos brinda elementos claves para analizar y comprender de mejor manera esta causa de inculpabilidad, al expresar una alteración clínicamente significativa de la cognición, se refiere, a cambios en los procesos mentales como el pensamiento, la memoria, la atención y la percepción que van más allá de las variaciones normales. Estos cambios son lo suficientemente severos como para causar malestar o dificultades significativas en la vida diaria

del individuo. Un trastorno mental puede afectar estos procesos de manera que altera la forma en que una persona interpreta la realidad o toma decisiones.

En resumen, la definición que nos brinda la OMS acerca de trastornos mentales nos indica que se trata de condiciones que afectan profundamente la forma en que una persona piensa, siente y actúa, causando dificultades significativas en su vida diaria que pueden llevar a diversos problemas, requiriendo intervención clínica para su tratamiento.

Acoplando esto al derecho, podemos decir que una persona cuyo estado mental sea desfavorable y que cometa un hecho antijurídico, sin saber lo que realiza o que tiene la percepción de la realidad alterada por su condición, no sería imputable, por ende, no se le puede atribuir una pena, pues no actúa con comprensión ni conocimiento. Como por ejemplo podemos nombrar a una persona que padece de esquizofrenia, enfermedad mental que se caracteriza por provocar perturbaciones en la afectividad y el pensamiento lo cual provoca una pérdida de contacto con la realidad, ideas delirantes y percepción alterada, esta persona en su delirio mental puede hurtar algún producto de un centro comercial sin saber que el hurto es un delito, de hecho no sabe ni porque hurta dicho producto, pues bien, este individuo no es adherente a una pena por su condición médica.

Según la legislación del Ecuador, a la persona que actúe de acuerdo a esta condición no se le hará responsable penalmente de sus actos. “En estos casos la o el juzgador dictará una medida de seguridad” (Código Orgánico Integral Penal, 2014, p. 18). Estas medidas están formalizadas en el mismo Código Orgánico Integral Penal.

4.9. Delito Informático

Los delitos informáticos son relativamente nuevos y al principio resultó difícil describirlos y clasificarlos adecuadamente. Sin embargo, es evidente que se ha trabajado para combatirlos y proteger la seguridad legal de los usuarios de sistemas informáticos a nivel mundial.

Hoy en día, los delitos informáticos representan un problema grave debido a la rápida evolución de la era digital. La tecnología avanza desenfrenadamente, lo cual dificulta crear leyes que regulen los ciberdelitos. Además, los perpetradores de estos delitos se adaptan continuamente a los avances tecnológicos y encuentran maneras de superar las medidas de seguridad diseñadas para prevenir estas conductas.

El delito informático o también conocido como ciberdelito, según la Real Academia de la Lengua española es: “Delito que se comete a través de internet” (Real Academia Española,

2024, p. 1). Esta definición que nos refiere la RAE, implica que un delito informático es cualquier acción ilícita que se realiza utilizando como medio principal o exclusivo las tecnologías de la información y la comunicación, especialmente la red de internet. La característica distintiva de un ciberdelito es que se lleva a cabo mediante el uso de dispositivos digitales y redes informáticas, aprovechando las vulnerabilidades tecnológicas o manipulando información digital de manera ilegal.

Este término realmente es algo nuevo, ya que se utilizó de manera imprecisa a finales de los años noventa cuando se comenzaron a dar los primeros problemas mediante el internet, y las naciones preocupadas por estos sucesos se reunieron en Lyon, Francia en donde se conformó el grupo denominado G8, el cual tenía el propósito de estudiar y analizar los casos recientes relacionados con la delincuencia que comenzó a obrar mediante el internet.

Como es de conocimiento general que de igual forma al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social han aparecido nuevos comportamientos dañinos para la sociedad. La doctrina ha denominado a este grupo de comportamientos como delitos informáticos o ciberdelitos.

Desde la doctrina se nos explica que es algo difícil dar un concepto para este tipo de delitos, puesto que es una terminología reciente, sin embargo, Julio Téllez Valdés nos indica que los delitos informáticos son: “conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin” (Téllez, 2008, p. 188).

Esto quiere decir que cualquier acción que encaje en la descripción de un delito (típica), que esté prohibida por la ley (antijurídica) y que pueda ser atribuida a alguien como responsable (culpable), donde las computadoras jueguen un papel central, ya sea como herramienta para cometer el delito o como objetivo del mismo, se considera un delito informático.

Desde otra perspectiva el abogado Michael Espinoza Coila, nos indica el delito informático desde varios puntos de vista de la siguiente manera:

> El Delito Informático (computer crime / computerkriminalität), es definido de manera (a) formal, como acción u omisión prohibida por la ley penal sobre delitos informáticos; (b) material, como conducta final que ofenden bienes jurídicos relacionados a las Tecnologías de la Información y la Comunicación (TIC), y (c) analítica, como conducta típica, antijuridica y culpable que tiene como medio u objeto de protección a las T.I.C (Espinoza, 2018, p. 238).

Son tres los puntos de vista que nos da acerca de esta problemática legal. Desde la perspectiva formal, se refiere a cualquier acción u omisión que esté explícitamente prohibido por la legislación penal relacionada con delitos informáticos. Por otro lado, cuando nos menciona el concepto de delito informático desde el punto de vista material, el autor se enfoca en cualquier comportamiento que cause daño a los derechos o bienes protegidos que estén relacionados con las TIC, como la privacidad de datos, la integridad de los sistemas informáticos, etc. Finalmente nos refiere que desde la figura analítica las TIC pueden ser tanto el medio para cometer el delito como el objetivo de protección legal.

Y como ultimo doctrinario tenemos al abogado Carlos Alcívar quien nos enseña que:

> Los delitos informáticos son aquellas actividades ilícitas que: (a) se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o (b) Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos) (Alcívar et al., 2015, pág 64).

Este doctrinario nos da dos posiciones, en la primera la informática es el medio o instrumento que se utiliza para llevar a cabo actividades ilícitas, es decir se lo realiza mediante computadoras u otros sistemas informáticos, como ejemplo de estos delitos tenemos la apropiación fraudulenta por medios electrónicos o la violación a la intimidad. Y desde la segunda posición, el objetivo del delito es específicamente causar daño a los sistemas informáticos, ya sea atacando la integridad de un sistema informático, impidiendo el acceso a los sistemas, etc.

Los tres autores coinciden en que los delitos informáticos implican el uso o afectación de tecnologías de la información y comunicación. Las definiciones varían en su énfasis, pero todas destacan en que los delitos informáticos pueden ser cometidos usando computadoras o sistemas informáticos y que estos pueden tener como objetico dañar o afectar a estos sistemas informáticos y los datos que contienen. Se destaca que las acciones cometidas por estos medios deben estar prohibidas en el sistema penal legal. Todos concuerdan en que este tipo de delitos afectan bienes jurídicos relacionados con las TIC, como la integridad de los sistemas y la seguridad de los mismos.

En resumen, los delitos informáticos abarcan una variada gama de actividades ilícitas que involucran las tecnologías de la información y la comunicación, ya sea utilizándolas como herramientas para cometer delitos o como objetivos de los mismos, siempre dentro del marco de lo prohibido por la ley penal.

Adentrándonos a la legislación ecuatoriana, no encontramos una definición como tal de los delitos informáticos, sin embargo, dentro de la Constitución de la República del Ecuador se protege el derecho a la protección de datos de carácter personal, a la intimidad personal y familiar, a la inviolabilidad y al secreto de la correspondencia física y virtual, ahora bien, los delitos informáticos atentan contra estos derechos constitucionales. Por ende, se puede decir que los delitos informáticos vendrían a ser las conductas ilícitas reguladas por la legislación que van en contra de derechos protegidos en la Constitución de la República del Ecuador.

En la actualidad, nuestro Código Orgánico Integral Penal vigente tipifica varios delitos informáticos en el Libro Primero Título Cuarto Capítulo Tercero: Delitos contra los Derechos del Buen Vivir Sección Tercera denominada: Delitos contra la seguridad de los activos de los sistemas de información y comunicación, claro que existen más de 30 delitos informáticos tipificados por la legislación ecuatoriana, mismos que se encuentran distribuidos por todo el cuerpo normativo. Siguiendo la realidad normativa, podemos decir que los delitos informáticos en el país, son aquellos que en la doctrina son expuestos desde dos puntos de vista, los que tienen como fin atacar la integridad de los sistemas informáticos y los que tienen como medio dichos sistemas informáticos para llegar a su cometido, como ejemplo de los primeros tenemos el ataque a la integridad de los sistemas informáticos y por su lado los segundos vendría a ser como ejemplo la revelación ilegal de datos.

Se evidencia un gran avance en el cometimiento de los delitos informáticos en el país, puesto que hoy en día en el país se usa en gran medida las TIC,

> Cinco tipos de estos ilícitos se han cometido con mayor frecuencia en el país. Estos son: la estafa en línea, violación a la intimidad, el acceso no consentido a un sistema informático, el ataque a la integridad de sistemas informáticos y la apropiación fraudulenta por medios electrónicos (El Comercio, 2022, p. 1).

En el aspecto del ciberespacio y de la ciberseguridad, el Ecuador ha experimentado un aumento significativo en el cometimiento de delitos informáticos. El comercio nos da los delitos informáticos que más se frecuentan en el país, este fenómeno criminal refleja el aumento de la dependencia del país en las tecnologías digitales y la necesidad urgente de reforzar las medidas de seguridad cibernética, incluyendo normas reguladoras dentro del sistema legal, además se evidencia la necesidad de mejorar e incentivar la educación digital y la concientización sobre las practicas seguras en línea.

Entrando a temas internacionales, la Oficina de las Naciones Unidas contra la Droga y el Delito nos menciona sobre el delito informático que: “En términos generales, el delito cibernético se puede describir como delitos ciber dependientes y delitos facilitados por medio de las Tecnologías de la Información y Comunicación” (UNDOC, 2024, p. 1). Las misma UNDOC nos explica que los delitos informáticos requieren de una infraestructura tecnológica, porque son dependientes de las TIC, es decir, son necesarias para el cometimiento de estas actividades, como por ejemplo una estafa en línea puede darse por medio de una computadora o un teléfono móvil, otros ejemplos de delitos facilitados por estos medios son: explotación sexual infantil en línea, apropiación fraudulenta por medios electrónicos, etc.

En el 2001 el Consejo de Europa crea el convenio de Budapest sobre la ciberdelincuencia: “En él se establecen normas de cooperación internacional para realizar procesos penales que ayuden a combatir los delitos informáticos” (Ortiz, 2019, p. 103) el Ecuador no es hasta el jueves 4 de julio del 2024 que la Asamblea Nacional aprueba la adhesión del país al Convenio de Budapest sobre Ciberdelincuencia. La ratificación de este convenio dará al Ecuador una guía en cuanto a la regulación de delitos informáticos.

Sabiendo todo esto podemos afirmar que los delitos informáticos, son aquellas conductas típicas, antijuridicas y culpables que se realizan a través de las tecnologías de la información y la comunicación como por ejemplo una estafa informática por medio de mensajes de texto y también son aquellas acciones de igual naturaleza atentan contra estos sistemas informáticos.

4.10. Elementos del tipo penal del Delito Informático

El tipo penal está formado de elementos tanto objetivos como subjetivos. En los elementos objetivos se resaltan los aspectos externos del comportamiento y consisten en: sujeto activo, sujeto pasivo, verbo rector, objetividad jurídica, objeto de la acción, resultado y sanción. Los elementos subjetivos son parte del sujeto activo, ya que, vendría siendo el estado psicológico de la persona al momento de realizar el hecho y consisten en el dolo o la culpa. Estos elementos suponen la existencia de un presupuesto legítimo, mismo que debe ser analizado por un juez para aplicar correctamente la ley.

4.10.1. Sujeto Activo en los delitos informáticos

Según la doctrina penal con respecto al sujeto activo, “se entiende por tal a quien realiza toda o una parte de la acción descrita por el tipo penal”. (Garrido, 1993, como se citó en Acuario, 2016,

pág. 15), entonces el sujeto activo en estos casos vendría siendo aquella persona ya sea natural o jurídica que realiza o comete los delitos informáticos.

"En la mayoría de tipos legales el sujeto activo puede ser cualquier persona, sin ninguna calidad o exigencia especial" (Albán, 2018, p. 147) se observa que el sujeto activo en casos de delitos informáticos puede ser cualquier persona, sin embargo, como estas conductas se realizan a través de medios informáticos como las computadoras o demás aparatos electrónicos se debe tener ciertas habilidades en el manejo de estos. Estas habilidades son las que les permiten engañar a sus víctimas y hacerles un daño a través de estos sistemas, ejemplo de estos pueden ser los denominados hackers. La diferencia de los sujetos activos en este tipo de delitos y los sujetos activos de los delitos comunes, es que estos realizan sus fechorías a través de los medios de información y comunicación. De igual manera se puede afirmar que cualquier persona natural o jurídica puede ser el sujeto activo de los delitos informáticos, como ejemplo puede ser una persona que mediante el uso de las redes sociales estafa en línea ofreciendo la venta de algún servicio y que al momento de entregar el producto solicitado este asegure el pago con anterioridad y de esta manera no entrega el servicio ofertado.

4.10.2. Sujeto Pasivo en los delitos informáticos

"El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo" (Acuario, 2016, p. 18). Siguiendo esta noción podemos referir que el sujeto pasivo es la víctima del delito, este es el ente sobre quien recae la conducta dañosa que es perpetrada por el sujeto activo.

Cualquier persona pueden ser sujetos pasivos de estas acciones, más sin embargo en la doctrina se nos refiere: "En ciertos tipos legales, para que haya tipicidad es necesario que éste reúna determinadas condiciones" (Albán, 2018, p. 105) este tipo de sujetos suelen ser denominados sujetos pasivos especiales.

Analizando todo esto podemos deducir que en los delitos informáticos cualquier persona ya sea natural como jurídica son propensas a ser sujetos pasivos a quienes se les vulnere o dañen derechos. Por ejemplo, la persona a la que le interceptan ilegalmente sus datos.

Con respecto a los sujetos pasivos especiales dentro de los delitos informáticos, los podemos encontrar en ciertos tipos delictivos, como lo son la pornografía infantil y actos ligados a la pornografía en menores de edad.

4.10.3. Verbo Rector de la Acción

El Dr. Ernesto Albán en su obra "Manual de Derecho Penal Ecuatoriano: Parte General" con respecto al verbo rector del delito, señala que: "Es el elemento central de la tipicidad, el que determina y delimita el acto (acción u omisión) ejecutado por la persona. Al ser, pues una conducta, el núcleo suele fijarse en la ley mediante un verbo" (Albán, 2018, p. 104).

Se puede decir entonces, con referencia a lo enseñado por el Dr. Albán, que el verbo rector es la acción específica que constituye el delito informático, como por ejemplo en el delito de revelación ilegal de datos, el verbo rector de esta conducta sería revelar. Revelar es la acción y quiere decir mostrar datos sin la autorización del propietario mediante medios electrónicos, violando el derecho de la intimidad.

4.10.4. Objetividad Jurídica de los delitos informáticos

> El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir -ya que constituye la razón de ser del delito- y no suele estar expresamente señalado en los tipos penales (Acuario, 2016, p. 20).

Siguiendo esta noción podemos decir que el objeto jurídico es el derecho protegido por la ley que se ve dañado por el delito informático. Estos delitos informáticos la mayoría de veces afectan derechos como la privacidad, la intimidad personal y familiar, el patrimonio y la propiedad privada. Sin embargo, como lo explica el Dr. Acuario, estos derechos no suelen estar explícitamente en el tipo penal como tal, pero son fundamentales para que se pueda formular un delito.

4.10.5. Objeto de la acción en delitos informáticos

"En ciertos delitos hace falta que el delito recaiga en determinado objeto material, que la ley expresamente exige" (Albán, 2018, p. 105). Esto nos hace referencia a un elemento material tangible en donde el daño recae. Basándonos en lo aportado por el Dr. Albán y relacionándolo con los delitos informáticos, el objeto de la acción por el cual recae la conducta, vendría siendo la información, los sistemas informáticos, documentos públicos o privados, grabaciones de voz, correos electrónicos, datos privados, etc.

4.10.6. Resultado en delitos informáticos

En resultado de una acción generalmente se entiende como las consecuencias que traen consigo la acción humana. Las consecuencias son sólo aquellas que directa o indirectamente están

relacionadas con hechos anteriores, en este caso delitos informáticos. Existen dos tipos de resultados, delitos que ponen en peligro los bienes jurídicos y delitos que dañan significativamente estos derechos.

En los delitos informáticos podemos encontrar estos dos tipos de resultado, el de peligro por ejemplo se ubicaría en el solo acceso no consentido a un sistema informático, ya que de esta manera se pone en peligro derechos como el de la privacidad y por otro lado un resultado de daño lo encontramos en el delito de violación a la intimidad, ya que en este delito se realizan acciones en donde se daña la intimidad de una persona, lastimando significativamente el bien jurídico protegido.

4.10.7. Sanción en delitos informáticos

> Al Derecho Penal, porque para él, y dejando aparte el debatido tema puramente teórico de la existencia de sanciones premiales, la sanción es la pena o castigo que la ley prevé para su aplicación a quienes incurran o hayan incurrido en una infracción punible (Ossorio, 2008, p. 870).

Partiendo de este concepto que nos da el Dr. Cabanellas de Torres, se analiza que la sanción es la consecuencia que la ley establece y que es aplicable para quienes cometen un delito. Este concepto es fundamental ya que establece las consecuencias legales de las conductas delictivas. A lo largo de la historia han surgido muchas clases y tipos de sanciones, pero en el Ecuador se las establece según el marco legal vigente en el Código Orgánico Integral Penal, en su artículo 51 dándonos una referencia a lo que es una pena de la siguiente manera: “La pena es una restricción a la libertad y a los derechos de las personas, como consecuencia jurídica de sus acciones u omisiones punibles. Se basa en una disposición legal e impuesta por una sentencia condenatoria ejecutoriada” (Código Orgánico Integral Penal, 2014, p. 26). En el cuerpo penal ecuatoriano evidenciamos un concepto de pena o sanción, la cual nos explica que es la restricción de la y derechos de las personas que delinquen ya sea por acción u omisión, estas penas están descritas en la ley y se las dictamina y ejecuta gracias a una sentencia condenatoria. De la misma forma el mismo cuerpo normativo nos da la clasificación de estas, dándonos como primeras a las penas privativas de la libertad, penas no privativas de la libertad y a las restrictivas de los derechos de propiedad.

Las penas privativas de la libertad solo pueden durar como máximo 40 años, en Colombia 50 años, en Perú hay un poco de diferencia puesto que en este tipo de penas tenemos que esta puede ser temporal o de cadena perpetua, en el caso de ser pena temporal la mínima es de 2 días

y la máxima de 35 años. Finalmente, en el caso de Costa Rica al igual que en Colombia es de 50 años. Además, a estas penas se les relacionan penas accesorias, que vendrían siendo las más comunes la multa, comiso penal, etc.

En el caso de los delitos informáticos dentro del Ecuador, se los sanciona con penas restrictivas de la libertad y si el juez lo considera con multas y en el caso de algunos delitos específicos, se impondrá la inhabilitación a los servidores públicos.

Los delitos informáticos en el país cuentan con penas restrictivas de la libertad que van desde un año a tres años, de tres a cinco años y las más graves de cinco a siete años, penas que van dentro de la sección de delitos informáticos establecidos como tal tácitamente dentro del Código Orgánico Integral Penal, ahora con respecto a los que son considerados delitos informáticos pero no se encuentran en esta sección específica, tenemos que las penas más leves son de uno a tres años en delitos como la apropiación fraudulenta de por medios electrónicos y las más grave es el delito de pornografía con utilización de niñas, niños o adolescentes con la pena de trece a diecisiete años.

4.10.8. Elemento subjetivo en delitos informáticos

Dentro de los elementos subjetivos del tipo penal, como ya se mencionó encontramos dos muy importantes, el dolo y la culpa.

Para definir lo que es el dolo nos adentraremos en la doctrina penal, específicamente en este caso nos guiaremos por lo que nos refiere el Dr. José Girón en su obra Teoría del Delito, él nos dice que el dolo: “Es conocimiento (saber) y voluntad (querer) de realizar el tipo objetivo. En el tipo doloso, hay coincidencia entre lo que el autor hace y lo que quiere” (Girón, 2021, p. 78). Partiendo de este concepto podemos analizar que los elementos del dolo son el conocimiento de que la conducta a punto de cometerse va en contra del ordenamiento jurídico y la voluntad es que de igual forma se quiere realizar el delito, pese a saber que está prohibido por la ley y que tiene una consecuencia jurídica para lo que se va a realizar. Podemos decir entonces que el dolo en el caso de los ciberdelitos es la intención del sujeto activo de cometer el delito informático sabiendo que esto tiene una consecuencia jurídica como una pena, un ejemplo de esto es el individuo que sabe que es prohibido interceptar datos voluntariamente lo realiza.

Acoplándonos a la legislación ecuatoriana vemos que este elemento esta normado en el artículo 26 del Código Orgánico Integral Penal de la siguiente manera: “Actúa con dolo la persona que,

conociendo los elementos objetivos del tipo penal, ejecuta voluntariamente la conducta" (Código Orgánico Integral Penal, 2014, p. 15).

El legislador ecuatoriano recoge la concepción doctrinaria acerca del dolo y lo plasma en la ley penal, diciendo que la persona actúa con dolo cuando conscientemente de que su acción es antijuridica y de forma voluntaria ejecuta la conducta. La capacidad cognitiva y volitiva dentro de este elemento es la más crucial e importante, porque si no existe la voluntad no existe delito.

Con respecto a la culpa o también llamada imprudencia no es más que el actuar de una persona sabiendo que se puede generar algún resultado dañino pero la gran y notoria diferencia es que no se tiene la voluntad de causar esa violación a la ley, este hecho puede ser tomado como un descuido, la culpa se frecuenta más en delitos de tránsito.

"En términos generales, puede decirse que actúa con culpa quien causa un daño sin propósito de hacerlo, pero obrando con imprudencia o negligentemente" (Ossorio, 2008, p. 244).

Según lo que nos explica el diccionario jurídico de Ossorio la culpa es la negligencia o descuido que un individuo tiene, pero sin la intención de cometer algún daño y sin embargo lo causa, un ejemplo de esto es que una persona mientras conduce revisa su teléfono celular y atropella a una persona, él sabía que esta conducta estaba mal sin embargo no tenía la voluntad de atropellar y causarle daño a alguien.

El legislador ecuatoriano nos establece que: "Actúa con culpa la persona que infringe el deber objetivo de cuidado, que personalmente le corresponde, produciendo un resultado dañoso" (Código Orgánico Integral Penal, 2014, p. 15), podemos ver que se asemeja a la doctrina y al ejemplo planteado anteriormente.

4.11. Tipos de Delitos Informáticos

La abogada Seidy Tixi en su estudio sobre delitos informáticos, nos presenta una clasificación de estos, basándose en la guía presentada por la Unión Internacional de Telecomunicaciones denominada El Ciberdelito: Guía para los Países en Desarrollo, este documento fue desarrollado por el Dr. Marco Gercke, el cual nos indica una clasificación completa de los ciberdelitos mismos que se describen así:

> **A.1. Acceso ilícito** (piratería de sistemas y programas): Entre estos se tiene la irrupción en sitios web protegidos con contraseña, la burla de la protección de contraseña en un computador, la utilización de equipos o programas para obtener una contraseña e irrumpir en el sistema informático, la creación de sitios web "falsos" para lograr que el

usuario revele su contraseña, la instalación por hardware y software de interceptores de teclado ("keyloggers").

A.2. Espionaje de datos, como software para explorar los puertos desprotegidos, software para burlar las medidas de protección, ingeniería social (Ej. "phishing"). Además, acceder a sistemas informáticos o a un dispositivo de almacenamiento y extraer la información.

A.3. Intervención ilícita, los delincuentes pueden intervenir las comunicaciones entre usuarios (cómo mensajes de correos electrónicos, interceptar transferencias de datos (cuando los usuarios suben datos a los servidores web o acceden a medios de almacenamiento externos por la web).

A.4. Manipulación de datos, como el borrado, supresión, alteración y restricción de acceso a datos.

A.5. Ataques contra la integridad del sistema, se encuentran los gusanos informáticos o software pernicioso que se reproduce de manera autónoma. Puede detener el funcionamiento informático y sobre utilizar los recursos del sistema. Además, los ataques de denegación de servicio (DoS).

Delitos relacionados con el contenido.

B.1. Material erótico o pornográfico (excluido la pornografía infantil), algunos países prohíben estrictamente el acceso e intercambio de material pornográfico.

B.2. Pornografía infantil, este tipo de pornografía es considerado de manera unánime como un acto criminal en cualquier lugar del mundo por ser un acto de explotación y abuso sexual. Se considera pornografía infantil a películas e imágenes que muestren niños en un contexto sexual.

B.3. Racismo, lenguaje ofensivo, exaltación de la violencia, personas o grupos radicales que utilizan los medios de comunicación masivos como Internet, páginas web o redes sociales para para divulgar información que genere odio o conflictos, actitudes racistas, homofóbicas, utilicen lenguaje ofensivo o impulsen a generar actos de violencia.

B.4. Delitos contra la religión, en algunos países se presentan normas jurídicas relacionadas a la religión y es un delito atentar contra la misma, como realizar

declaraciones antirreligiosas, crear contenido que genere polémica o burla a los aspectos y creencias religiosas.

B.5. Juego ilegales y juegos en línea, permiten cometer ciertos delitos, como el intercambio y presentación de pornografía infantil, realizar fraudes, apuestas ilícitas, difamaciones o calumnias, evadir las normas o prohibiciones de juego de acuerdo a las leyes de cada país. Los casinos también pueden llegar a utilizarse para lavar dinero o financiar el terrorismo.

B.6. Difamación e información falsa, publicar información falsa, escribir mensajes difamatorios o calumnias, revelar información confidencial como secretos de Estado o información comercial confidencial.

B.7. Correo basura y amenazas conexas, se entiende como el envío masivo de mensajes masivos no solicitados. Los infractores envían millones de mensajes de correo electrónico a usuarios, en los que presentan anuncios o software pernicioso (botnets).

B.9. Otras formas de contenido ilícito, como solicitar, ofrecer e incitar al crimen, la venta ilegal de productos, información e instrucciones para actos ilícitos (Ej. para construir explosivos o armas).

Delitos en materia de derechos de autor y de marcas

C.1. Delitos en materia de derechos de autor y de marcas, como sistemas de intercambio de archivos, de programas informáticos, archivos y temas musicales protegidos con derechos de autor. También la elusión de los sistemas de gestión de derechos en el ámbito digital.

C.2. Delitos en materia de marcas, la utilización de marcas en actividades delictivas con el propósito de engañar a las víctimas. Además, los delitos en materia de dominios y nombres.

Delitos informáticos

D.1. Fraude informático, como subasta en línea (ofrecer mercancías no disponibles, adquirir mercancías sin pagar por ellas). Estafa nigeriana (solicitan ayuda a los destinatarios para transferir sumas de dinero).

D.2. Falsificación informática, se encuentra el fraude informático, manipular imágenes electrónicas (por ejemplo, imágenes aportadas como pruebas materiales en los tribunales) y la alteración de documentos.

D.3. Robo de identidad, interacción con la información obtenida antes de utilizarla en el marco de una actividad delictiva, como ocurre con la venta de ese tipo de información (Ej. se venden listas de tarjetas de crédito a un precio determinado). También la utilización de la información relativa a la identidad en relación con una actividad delictiva (Ej. la falsificación de documentos de identidad o el fraude de las tarjetas de crédito).

D. 4. Utilización indebida de dispositivos, Pueden encontrarse herramientas que simplifican el cometer delitos informáticos como el correo basura, las descargas de archivos, que se utilizan para cometer ataques por denegación de servicio, diseñar virus informáticos, desencriptar información o acceder en forma ilegal a sistemas informáticos (Gercke, 2009, como se citó en Tixi, 2022, págs. 4-5-6)

Esta clasificación ofrece una visión integral de los diferentes tipos de delitos informáticos, destacando la diversidad y complejidad de las amenazas en el ciberespacio. Comprender estas categorías es esencial para desarrollar estrategias efectivas de prevención y respuesta ante estos delitos.

Con respecto a los delitos informáticos en el contexto de la legislación ecuatoriana los encontramos descritos y tipificados en el Código Orgánico Integral Penal, dentro del Libro Primero Título Cuarto Capítulo Tercero: Delitos contra los Derechos del Buen Vivir Sección Tercera denominada: Delitos contra la seguridad de los activos de los sistemas de información y comunicación, en esta sección encontramos siete delitos informáticos y unas breves definiciones para comprender más a fondo estas conductas dañosas, sin embargo se sabe que dentro del cuerpo penal existen alrededor de 30 ciberdelitos más, pero no están descritos exactamente en esta sección en específico, sino que los encontramos dispersos por todo el Código, pero en esta investigación analizaremos solo los tipos penales de la sección nombrada anteriormente.

En Colombia el 5 de enero de 2009 el Congreso de Colombia legisla la Ley 1273:

> Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan

> integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones (Congreso de Colombia, 2009, p. 1).

Esta ley tipificó como delitos una serie de conductas relacionadas con el manejo de información personal, ya que en relación a datos de carácter personal es en donde más atacan los ciberdelincuentes, por este motivo es de gran importancia que las personas naturales y jurídicas tengan garantías en la ley para poder hacer valer sus derechos y evitar caer en este tipo de ciberdelitos.

En el Perú el 22 de octubre del 2013 se publica en el Diario Oficial El Peruano la Ley 30096, Ley de delitos informáticos que regula y previene lo que vendría siendo las conductas dañinas hacia la ciudadanía mediante el uso de las TICS, con esta ley se pretende prevenir y sancionar las conductas ilícitas que atentan contra la información y sistemas informáticos.

En cuanto a legislación informática dentro de Costa Rica se logra apreciar el esfuerzo que ha hecho el país por aplicar normas que regulen lo que vendría siendo las relaciones en el ciberespacio, como por ejemplo en el Código Penal de este país, se tipifica y sanciona algunos delitos informáticos. De esta manera se previene la delincuencia informática y se garantiza una mejor seguridad para los usuarios de este tipo de tecnologías.

Los delitos informáticos tipificados en el Ecuador son los siguientes:

> **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, base 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 (Código Orgánico Integral Penal, 2014, p. 77).

Este delito se comete cuando una persona, con el fin de beneficiarse a sí misma o a un tercero, divulga información contenida en base de datos, archivos o sistemas electrónicos, violando intencionalmente la privacidad y el secreto de las personas. De esta manera el cuerpo normativo establece un marco claro y preciso para la protección de la privacidad y la confidencialidad de

la información contenida en bases de datos. Al penalizar la revelación no autorizada de datos, se busca mantener la integridad de la información personal y sancionar a aquellos que, aprovechando su acceso a información sensible, violen los derechos de privacidad e intimidad de las personas. Este delito tiene relación con el tipo penal tipificado en el Código Penal Colombiano denominado Violación de datos personales.

> **Art. 269-F.- Violación de datos personales.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Congreso de Colombia, 2000, p. 130).

En este caso podemos asegurar que estos delitos tienen similitudes, como por ejemplo ambos artículos buscan proteger la información personal y los datos contenidos en archivos, bases de datos, o sistemas electrónicos, ambos penalizan la revelación o divulgación de datos y en ambos casos el delito puede cometerse en provecho propio o de un tercero.

En cuanto a las diferencias podemos referir que el artículo 269-F de Colombia penaliza una amplia gama de conductas, incluyendo la obtención, compilación, sustracción, oferta, venta, intercambio, envió, compra, intercepción, modificación o empleo de datos personales y por su parte el artículo 229 de Ecuador se enfoca principalmente en la revelación de información registrada en ficheros, archivos, bases de datos o sistemas electrónicos, y en la violación del secreto, la intimidad y la privacidad de las personas.

Respecto a las sanciones en la legislación colombiana se establece una pena prisión de 48 a 96 meses (4 a 8 años) y multas de 100 a 1000 salarios mínimos legales mensuales vigentes, tomando en consideración que el salario mínimo legal del vecino país es de un millón trescientos mil pesos colombianos que su equivalente en dólares sería trescientos veinticinco con treinta y nueve, en total las multas serian desde ciento treinta millones a trece mil millones de pesos colombianos.

En cambio, el legislador ecuatoriano propone una pena privativa de libertad de 1 a 3 años. Y en caso de sanción con multa, según lo establecido en el COIP, esta sería de 4 a 10 salarios básicos unificados del trabajador en general.

Aunque ambos artículos tratan sobre la protección de datos personales y la penalización de conductas relacionadas con el uso no autorizado de dichos datos, se diferencian en el alcance de las conductas penalizadas y en las sanciones establecidas. El Art. 269-F del Código Penal Colombiano es más amplio y abarca una mayor variedad de acciones delictivas, mientras que el Art. 229 solo sanciona la revelación de información con la intención y voluntad de violar la intimidad y privacidad personal. Por lo tanto, aunque van al fondo de la misma cuestión de proteger los datos personales, lo hacen desde enfoques ligeramente distintos.

Relacionándolo con los delitos tipificados en la Ley 30009 del Perú, encontramos que en esta legislación se tipifica este delito, pero con una denominación diferente a la del Ecuador y Colombia, el delito se encuentra como Tráfico ilegal de datos mismo que se encuentra en el capítulo IV delitos informáticos contra la intimidad y el secreto de las comunicaciones y se describe así:

> **Artículo 6. Tráfico ilegal de datos:** El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años (Congreso de la República del Perú, 2013, p. 3).

Este delito se asimila al tipo penal de Ecuador ya que estos artículos tratan sobre la protección de datos personales y la penalización del tráfico y revelación ilegal de dichos datos en Perú y Ecuador. Ambos artículos buscan proteger los datos personales y la información contenida en bases de datos. De igual manera mediante estos se busca penalizar el uso indebido de datos personales, ya sea mediante su creación, uso, comercialización, tráfico, venta, o revelación sin autorización. Los dos artículos se aplican a datos personales relacionados con cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera, etc.

El tipo penal peruano penaliza la creación, ingreso o uso indebido de bases de datos para comercializar, traficar, vender, promover, favorecer o facilitar información personal. La pena es de tres a cinco años de prisión.

En cambio, Ecuador penaliza la revelación de información contenida en bases de datos y la violación del secreto, la intimidad y la privacidad de las personas. La pena es de uno a tres años

de prisión, y de tres a cinco años si el delito es cometido por servidores públicos, empleados bancarios, o similares.

Aunque ambos artículos buscan proteger los datos personales y penalizar su uso indebido, lo hacen desde enfoques diferentes:

El artículo de la normativa peruana se centra en el tráfico y comercialización de datos, penalizando una variedad de conductas relacionadas con el uso indebido de bases de datos.

Por su parte la norma penal del Ecuador se centra en la revelación de información y la violación de la privacidad, con un enfoque más específico en proteger el secreto y la intimidad de las personas.

Por lo tanto, aunque ambos van al fondo de la misma cuestión de proteger los datos personales, abordan el problema desde diferentes ángulos y con distintas especificidades en las conductas penalizadas y las sanciones establecidas.

Ahora por la parte de la legislación costarricense encontramos en el artículo 196 bis del Código Penal, un delito similar al descrito anteriormente y se lo describe de la siguiente forma:

> **Artículo 196 bis. - Violación de datos personales.** Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.
>
> La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:
>
> a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
>
> b) La información vulnerada corresponda a un menor de edad o incapaz.
>
> c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

> No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.
>
> Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley (Asamblea legislativa de la república de Costa Rica, 1970, p. 75).

En cuanto a las semejanzas entre los delitos ecuatorianos y costarricenses, ambos artículos buscan proteger los datos personales almacenados en sistemas o redes informáticas, así como en otros contenedores electrónicos, penalizando el acceso, uso y revelación no autorizada de datos personales y otras acciones que interfieran con la privacidad y la intimidad de las personas. Además, prevén sanciones más severas para ciertos grupos de personas, como administradores de sistemas y servidores públicos, y en situaciones específicas, como cuando la información vulnerada corresponde a menores de edad o incapacitados.

Por otro lado, haciendo referencia a las diferencias, el Artículo 196 bis penaliza más conductas como las relacionadas con el manejo indebido de datos personales, incluyendo la copia, transmisión, publicación, difusión, recopilación, venta y compra de datos sin autorización, además de considerar el tratamiento no autorizado de imágenes o datos. Por otro lado, el Artículo 229 se centra principalmente en la revelación ilegal de información registrada en bases de datos.

En el ámbito de aplicación, el Artículo 196 bis incluye excepciones para la publicación de información de interés público, documentos públicos, y datos en registros públicos de acceso irrestricto, además de exceptuar la recopilación y uso de información por entidades financieras supervisadas. El Artículo 229 no menciona excepciones específicas relacionadas con la publicación o recopilación de información de interés público o por entidades financieras.

Respecto a la gravedad de las sanciones, el Artículo 196 bis establece una pena de prisión de uno a tres años para la mayoría de las conductas, y de dos a cuatro años para conductas agravadas, como las realizadas por administradores de sistemas o cuando la información vulnerada corresponde a menores de edad o incapaces. El Artículo 229 establece una pena de prisión de uno a tres años, con una agravante de tres a cinco años si la conducta es cometida por servidores públicos o empleados bancarios.

Ambos artículos abordan la protección de los datos personales y la penalización de su uso indebido, pero desde enfoques ligeramente diferentes: el Artículo 196 bis tiene un enfoque más amplio y abarca una variedad de acciones relacionadas con el manejo indebido de datos personales, estableciendo también varias excepciones importantes, mientras que el Artículo 229 se centra en la revelación ilegal de información y la violación de la privacidad, con sanciones específicas para ciertos tipos de infractores y situaciones agravantes. En resumen, los dos artículos van al fondo de la misma cuestión de proteger los datos personales y la privacidad de las personas, pero lo hacen desde diferentes perspectivas y con distintas especificaciones en las conductas penalizadas y las sanciones establecidas.

El segundo delito informático del Ecuador es:

> **Art. 230.- Interceptación ilegal de datos. -** Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.
>
> 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.
>
> 3. La persona que posea, venda, distribuya o, de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior.
>
> 4. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
>
> 5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos, o programas o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Código Orgánico Integral Penal, 2014, p. 78).

El Artículo 230 del Código Orgánico Integral Penal de Ecuador define y penaliza una variedad de conductas relacionadas con la interceptación y manipulación ilegal de datos y sistemas informáticos, estableciendo una pena de prisión de tres a cinco años para las personas que realicen las siguientes conductas:

Interceptación de Contenidos Digitales: Penaliza la interceptación, escuchar, desviar, grabar u observar, sin orden judicial previa, el contenido digital en su origen, destino o dentro de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales.

Esta conducta busca proteger la confidencialidad y privacidad de las comunicaciones digitales y datos en tránsito, destacando la ausencia de orden judicial y la realización de la conducta en provecho propio o de un tercero.

Creación y Distribución de Contenidos Digitales Fraudulentos: Penaliza diseñar, desarrollar, ejecutar, producir, programar o enviar contenido digital, códigos de acceso o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes, así como la modificación del sistema de resolución de nombres de dominio (DNS) para inducir a una persona a ingresar a un sitio de internet diferente al que quiere acceder. Esta conducta combate el phishing, la creación de sitios web fraudulentos y otras formas de engaño en línea, subrayando la ilegitimidad de la acción y la intención de inducir a error a la víctima.

Difusión de Contenidos Destinados a la Interceptación Ilegal: Penaliza poseer, vender, distribuir o diseminar programas o contenidos digitales destinados a causar los efectos descritos en el numeral anterior. Esta conducta previene la distribución y uso de herramientas destinadas a cometer fraudes digitales y otras formas de interceptación ilegal, destacando la intención de causar efectos ilegales y la posesión o distribución de los contenidos.

Clonación y Comercialización de Información de Tarjetas: Penaliza copiar, clonar o comercializar información contenida en bandas magnéticas, chips u otros dispositivos electrónicos soportados en tarjetas de crédito, débito, pago o similares. Esta conducta protege los datos financieros y evita fraudes relacionados con tarjetas de pago, subrayando la acción de clonar o comercializar información de dispositivos electrónicos de pago.

Producción y Distribución de Dispositivos para Fraude: Penaliza producir, fabricar, distribuir, poseer o facilitar materiales, dispositivos electrónicos, programas o sistemas informáticos destinados a cometer el delito descrito en el inciso anterior. Esta conducta previene la fabricación y distribución de herramientas destinadas a cometer fraudes electrónicos y otros

delitos informáticos, destacando la intención de usar o facilitar el uso de dispositivos o programas para cometer delitos. El Artículo 230 del COIP trata varias conductas relacionadas con la interceptación y manipulación ilegal de datos y sistemas informáticos. Su enfoque está en proteger la privacidad de las comunicaciones digitales, la integridad de los sistemas informáticos, y la seguridad de los datos financieros. Las penas de tres a cinco años de prisión reflejan la gravedad con la que se considera este tipo de delitos en Ecuador. Las conductas descritas son claras y detalladas, lo que permite una aplicación efectiva de la ley contra diversas formas de delitos informáticos.

Delito similar en Colombia es el artículo 269-C que dice:

> **Art. 269-C.- Interceptación de datos informáticos.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses (Congreso de Colombia, 2000, p. 130).

Primero se destaca en ambos tipos penales que la persona que comete esta conducta debe de realizarlo sin una orden judicial previa, destacando que este hecho vendría siendo ilegal. Ambos artículos tienen como objetivo proteger la integridad y confidencialidad de los datos y sistemas informáticos, penalizando conductas relacionadas con la interceptación y manipulación de datos sin autorización. En los dos se establecen penas de prisión para los infractores, aunque varían en la duración de las penas. Los dos penalizan la interceptación de datos informáticos en su origen, destino o dentro de un sistema informático. Sin embargo, existen diferencias en la amplitud de conductas penalizadas y la especificidad de las mismas. El Artículo 269-C del Código Penal de Colombia se centra específicamente en la interceptación de datos informáticos y emisiones electromagnéticas provenientes de sistemas informáticos, con una pena de prisión de treinta y seis (36) a setenta y dos (72) meses (3 a 6 años). En contraste, el Artículo 230 del Código Orgánico Integral Penal del Ecuador especifica más, incluyendo escuchar, desviación, grabación, observación de contenido digital, la creación y distribución de contenidos digitales fraudulentos. También penaliza la copia y clonación de información de tarjetas de crédito y la fabricación de dispositivos para cometer fraudes electrónicos, con penas de tres a cinco años de prisión. En resumen, aunque ambos artículos van al fondo de la misma cuestión de proteger la integridad y confidencialidad de los datos informáticos y sistemas electrónicos de accesos no autorizados y manipulaciones ilegales, lo hacen desde enfoques ligeramente diferentes. El

Artículo 269-C del Código Penal de Colombia se centra exclusivamente en la interceptación de datos y emisiones electromagnéticas sin autorización, con una pena específica de prisión. En cambio, el Artículo 230 del Código Orgánico Integral Penal de Ecuador tiene un enfoque más amplio que abarca no solo la interceptación de datos, sino también otras formas de manipulación y fraude digital, con una variedad de conductas penalizadas y penas de prisión. Así, el artículo ecuatoriano abarca un espectro más amplio de conductas ilegales relacionadas con los delitos informáticos.

En Perú existe el tipo penal en cuestión con la misma denominación que tiene Colombia dentro del Artículo 7 de la Ley 30096 y se lo describe de la siguiente manera:

> **Artículo 7. Interceptación de datos informáticos:** El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
>
> La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
>
> La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales (Congreso de la República del Perú, 2013, p. 3).

Los Artículos 7 de la Ley de delitos Informáticos Perú y 230 del Código Orgánico Integral Penal del Ecuador tienen como objetivo proteger la integridad y confidencialidad de los datos y sistemas informáticos, penalizando conductas relacionadas con la interceptación no autorizada. De igual forma ambas legislaciones establecen penas de prisión para los infractores, aunque varían en la duración y severidad de las penas. Los dos artículos penalizan la interceptación de datos informáticos en su origen, destino o dentro de un sistema informático, incluyendo señales electromagnéticas provenientes de dichos sistemas. Sin embargo, existen diferencias en la amplitud de conductas penalizadas y la especificidad de las mismas.

El Artículo 7 de la Ley 30096 de Perú se centra específicamente en la interceptación de datos informáticos en transmisiones no públicas y las emisiones electromagnéticas, estableciendo

penas más severas para casos que comprometan información clasificada o la seguridad nacional. Por su parte, el Artículo 230 del Código Orgánico Integral Penal de Ecuador describe más conductas, incluyendo no solo la interceptación, sino también la escucha, desviación, grabación, observación de contenido digital, y la creación y distribución de contenidos digitales fraudulentos. También penaliza la copia y clonación de información de tarjetas de crédito y la fabricación de dispositivos para cometer fraudes electrónicos.

Respecto a las penas de prisión, el Artículo 7 de Perú establece una pena de prisión de tres a seis años para la interceptación de datos informáticos, aumentando a cinco a ocho años si la información es clasificada como secreta y de ocho a diez años si compromete la seguridad nacional. Por otro lado, el Artículo 230 de Ecuador establece una pena de prisión de tres a cinco años para las conductas descritas, sin especificar agravantes basadas en la naturaleza de la información interceptada. Los dos articulados buscan proteger la privacidad, la integridad y confidencialidad de los datos informáticos y sistemas electrónicos de accesos no autorizados, además luchan contra manipulaciones ilegales de los mismos.

Con la legislación de Costa Rica podemos decir que el delito de Interceptación Ilegal de Datos se relaciona con el delito ya antes mencionado de Violación de Datos, o también con el delito de Espionaje Informático en el artículo 231 del Código Penal.

> **Artículo 231.- Espionaje informático**: Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio (Asamblea legislativa de la república de Costa Rica, 1970, p. 89)

Se lo relaciona con el artículo 230 del COIP porque este tipo penal cubre una amplia gama de conductas que pueden ser consideradas como espionaje informático, incluyendo la interceptación de datos y el uso de software para obtener acceso no autorizado a información confidencial. Por lo tanto, el espionaje informático en ecuador podría ser acusado bajo este artículo, considerando las conductas específicas descritas en sus incisos.

Luego tenemos el artículo 231 del COIP en el Ecuador, en donde nos establece otro delito de naturaleza informática, que se describe así:

> **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 (Código Orgánico Integral Penal, 2014, p. 78).

La norma anteriormente citada describe dos tipos de conductas delictivas: alteración, manipulación o modificación de sistemas informáticos y la facilitación de datos bancarios. En cuanto a la alteración, manipulación o modificación de sistemas informáticos, la persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programas o sistemas informáticos, telemáticos o mensajes de datos para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona. Respecto a la facilitación de datos bancarios, 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. Un elemento subjetivo del tipo penal es el ánimo de lucro, que implica la intención de obtener un beneficio económico. Los medios comisivos incluyen la utilización de tecnologías de la información y la comunicación, como sistemas informáticos, programas, y mensajes de datos, para cometer el delito. El resultado de estas acciones es la transferencia o apropiación no consentida de un activo patrimonial en perjuicio de la víctima o de un tercero. La sanción establecida es una pena privativa de libertad de tres a cinco años. En cuanto a la tipicidad objetiva, la acción típica consiste en alterar, manipular o modificar sistemas informáticos con el fin de lograr una transferencia no consentida de activos patrimoniales. También se incluye la facilitación de datos bancarios para obtener ilegítimamente dichos activos. El uso de programas, sistemas informáticos, telemáticos y mensajes de datos es esencial para la configuración del tipo penal. En cuanto a la tipicidad subjetiva, el ánimo de lucro es fundamental y debe demostrarse que el autor actuó con la intención de obtener un beneficio económico. Además del ánimo de lucro, debe existir una intención fraudulenta de apropiarse de activos patrimoniales sin el consentimiento de su legítimo propietario. El bien jurídico protegido es el patrimonio de las personas, asegurando que los activos patrimoniales no sean transferidos o apropiados sin el consentimiento del titular. La norma agrava la conducta cuando se facilita o proporciona datos bancarios para la comisión del delito, indicando una colaboración activa en el fraude.

En Colombia encontramos este tipo penal con otra descripción pero que de igual manera se relaciona con el delito tipificado en el Ecuador, el mismo se encuentra descrito de la siguiente manera:

> **Art. 269-J.- Transferencia no consentida de activos.** El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.
>
> La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad (Congreso de Colombia, 2000, p. 132).

Estos delitos protegen al patrimonio de los delitos informáticos, estos se relacionan entre sí, pero con algunas ligeras diferencias.

Ambos artículos, el 231 del Código Orgánico Integral Penal (COIP) de Ecuador y el 269 del Código Penal de Colombia, tipifican conductas relacionadas con la manipulación informática destinada a obtener la transferencia no consentida de activos patrimoniales. Aunque comparten similitudes en sus objetivos y elementos, presentan diferencias notables en su redacción, alcance y sanciones, reflejando enfoques legislativos distintos en la protección del patrimonio frente a los delitos informáticos.

Estos artículos penalizan la manipulación informática con el propósito de lograr la transferencia no consentida de activos patrimoniales. Específicamente, el artículo 231 del COIP se enfoca en la alteración, manipulación o modificación de sistemas informáticos y mensajes de datos, así como la facilitación de datos bancarios para obtener activos de manera ilegítima. En cambio, el artículo 269 del Código Penal colombiano abarca manipulaciones informáticas o artificios semejantes de manera más general. Ambos tipos penales requieren el ánimo de lucro como elemento subjetivo esencial, implicando que la intención del autor es obtener un beneficio económico mediante la conducta delictiva.

En cuanto a las diferencias, el artículo 231 del COIP describe de manera específica la alteración de sistemas informáticos y mensajes de datos, y la facilitación de datos bancarios para obtener activos de manera ilegítima. En contraste, el artículo 269 del Código Penal colombiano tiene un enfoque más amplio, penalizando cualquier manipulación informática o artificio semejante que conduzca a la transferencia no consentida de activos. En términos de penas y agravantes, en Colombia, la pena de prisión para estas conductas es de 48 a 120 meses (4 a 10 años), junto con multas adicionales. Esta sanción puede incrementarse si el perjuicio económico supera ciertos umbrales, indicando un agravamiento basado en la cuantía del daño. Además, la legislación colombiana incluye una extensión del delito para abarcar la fabricación y facilitación de software malicioso. En Ecuador, la pena establecida es de tres a cinco años de prisión, y se prevé una agravante específica para la facilitación de datos bancarios, señalando una colaboración activa en el fraude. La legislación ecuatoriana no incluye especificaciones sobre la cuantía del perjuicio para el incremento de la sanción, centrándose más en la naturaleza de la conducta delictiva.

Los dos artículos reflejan una preocupación legislativa por proteger el patrimonio frente a manipulaciones informáticas y asegurar que las tecnologías de la información no se utilicen para perjudicar económicamente a las personas.

Aunque ambos artículos persiguen el mismo objetivo de proteger el patrimonio y la integridad de las transacciones financieras en el entorno digital, las diferencias en la redacción, el detalle y la severidad de las penas reflejan enfoques legislativos ligeramente diferentes entre Ecuador y Colombia. La mayor especificidad y el rango más amplio de sanciones en la legislación colombiana ofrecen una mayor flexibilidad para abordar diversas formas de delitos informáticos, mientras que la legislación ecuatoriana proporciona una protección enfocada y específica contra conductas claramente definidas en su normativa penal.

Con respecto al Perú, podríamos decir que el delito de Fraude Informático cumple el rol que en la legislación ecuatoriana y colombiana cumple el delito de transferencia electrónica de activo patrimonial. Este delito se describe así:

> **Artículo 8. Fraude informático**: El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un

sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social (Congreso de la República del Perú, 2013, pp. 3-4).

El Artículo 8 de la normativa legal peruana aborda específicamente el fraude informático, incluyendo la transferencia no consentida de activos patrimoniales mediante manipulación informática, específicamente en donde nos dice: "El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero" (Congreso de la República del Perú, 2013, pp. 3-4) en esta parte se puede entender como provecho ilícito la transferencia de activos. Este artículo establece una pena privativa de libertad de tres a ocho años, reflejando la gravedad del delito y el daño económico que puede causar a las víctimas. Mientras que en el Ecuador a la transferencia electrónica de activo patrimonial se la sanciona con prisión de tres a cinco años.

En un caso de transferencia no consentida de activos, es crucial que la acusación demuestre claramente la manipulación informática utilizada por el delincuente y el perjuicio económico sufrido por la víctima. La legislación peruana proporciona un marco adecuado para procesar estos delitos, asegurando que los responsables enfrenten sanciones proporcionales a la gravedad de sus acciones.

En Costa Rica no existe este delito informático.

El siguiente artículo del Código Orgánico Integral Penal tipifica otro delito informático de la siguiente manera:

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

> Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.
>
> Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad (Código Orgánico Integral Penal, 2014, p. 78).

Este artículo se centra en las acciones que destruyan, dañan, alteran o interfieren en el funcionamiento de sistemas informáticos, dispositivos electrónicos o infraestructura tecnológica. La pena de tres a cinco años de prisión se aplica tanto a quienes directamente causan estos daños como a quienes diseñan o distribuyen herramientas maliciosas destinadas a estos fines. La gravedad del delito aumenta a cinco a siete años de prisión si el ataque afecta a sistemas destinados a servicios públicos o seguridad ciudadana. Este enfoque subraya la importancia de proteger la integridad de la infraestructura tecnológica esencial para el funcionamiento adecuado de la sociedad y la seguridad nacional, disuadiendo así ataques maliciosos que pueden tener consecuencias devastadoras.

En la realidad de Colombia existen dos tipos penales que se relacionan con este y serían los siguientes:

> **Art. 269-B.- Obstaculización ilegítima de sistema informático o red de telecomunicación.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
>
> **Art. 269-D.- Daño Informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2000, p. 130)

Los Artículos 269-B y 269-D del Código Penal de Colombia y el Artículo 232 del Código Orgánico Integral Penal de Ecuador comparten la intención de proteger la integridad y funcionalidad de los sistemas y datos informáticos. Todos estos artículos abordan conductas que afectan negativamente a sistemas informáticos, ya sea mediante la obstrucción del acceso o el daño directo a datos y sistemas. En cada caso, se establecen penas de prisión para quienes actúen sin autorización, sanciones que buscan prevenir y castigar las interferencias y daños causados a la infraestructura tecnológica. Los artículos reflejan una preocupación común por salvaguardar el funcionamiento adecuado y la integridad de los sistemas informáticos y las redes de telecomunicaciones, imponiendo penas severas para mantener la seguridad y estabilidad tecnológica.

El Artículo 269-B del Código Penal colombiano trata sobre la obstaculización ilegítima de sistemas informáticos o redes de telecomunicaciones. Penaliza a quienes impidan o dificulten el acceso y funcionamiento de sistemas informáticos, datos contenidos por los mismos o redes de telecomunicaciones sin la debida autorización, imponiendo penas de prisión de 48 a 96 meses (4 a 8 años) y multas de 100 a 1000 salarios mínimos legales mensuales vigentes. Este artículo se enfoca en las acciones que interfieren en el acceso normal a los sistemas y redes.

Ahora, el Artículo 269-D del Código Penal de Colombia se ocupa del daño informático, penalizando a quienes destruyan, dañen, borren, deterioren, alteren o supriman datos informáticos o sistemas de tratamiento de información sin autorización. También establece penas de prisión de 48 a 96 meses (4 a 8 años) igual que en el tipo penal anterior y multas de igual forma de 100 a 1000 salarios mínimos legales mensuales vigentes. Este artículo abarca tanto la destrucción de datos como la alteración de los sistemas que procesan esos datos.

Por su parte el tipo penal del artículo 232 del Código Orgánico Integral Penal del Ecuador, sanciona la conducta delictiva con una pena privativa de libertad de tres a cinco años. También, el Artículo 232 del COIP trata sobre más acciones ilegales que incluyen tanto la destrucción directa como la interrupción del funcionamiento de sistemas, así como la distribución de software malicioso. Por su parte, el Artículo 269-B y el Artículo 269-D de Colombia se centran más en la obstrucción del acceso y el daño a los datos o sistemas informáticos, respectivamente. La principal diferencia radica en el alcance y la gravedad de las sanciones, por ejemplo el artículo 232 impone penas más severas cuando el ataque afecta a bienes críticos para el servicio público o la seguridad.

En resumen, estos artículos reflejan un enfoque robusto en la protección de sistemas informáticos, abordando desde la obstrucción del acceso hasta el daño y la distribución de software malicioso. Las sanciones severas están diseñadas para disuadir y penalizar a quienes interfieren con la funcionalidad y la integridad de sistemas tecnológicos esenciales.

De igual manera se guarda relación con el siguiente artículo establecido en el Código Penal de Colombia:

> **Art. 269-E.- Uso de software malicioso:** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2000, pp. 130-131).

Existe una gran similitud entre Colombia y Perú en el contexto de estos dos delitos, ya que, se tipifica este delito en dos tipos penales diferentes, caso contrario a Ecuador en donde está en uno solo, los ciberdelitos de Perú dicen:

> **Artículo 3. Atentado contra la integridad de datos informáticos:** El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.
>
> **Artículo 4. Atentado contra la integridad de sistemas informáticos:** El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa (Congreso de la República del Perú, 2013, p. 2).

La diferencia radica en la descripción y del tipo penal y en algunos verbos rectores, pero en si las conductas descritas llegan a lo mismo, sancionar delitos que atenten en contra de información digital y sistemas informáticos que contengan dicha información, otra diferencia notoria entre estos delitos y el de Ecuador es la forma de sancionar, el legislador ecuatoriano considera que la sanción para este delito basta de 3 a 4 años de pena privativa de libertad, con

una agravante en donde si la infracción recae sobre un bien informático que tenga como finalidad la prestación de un servicio público o vinculado con la seguridad ciudadana la pena aumentará de 5 a 7 años de pena privativa de libertad.

En el caso de los delitos que constan en la norma peruana observamos que las penas en ambos casos van de 3 a 6 años y además se les agrega una multa de ochenta a ciento veinte días de multa, que vendría a ser, considerando el sueldo legal en este país de 1025 soles, la deuda sería de 3564,8 soles a 5347,2 soles, que en dólares americanos son $947,42 a $1421,12 dólares americanos.

De igual forma se relaciona claramente con otro artículo de esta ley, en donde por separado se describe la producción de aplicaciones dañinas o virus para cometer estos delitos.

> **Artículo 10. Abuso de mecanismos y dispositivos informáticos:** El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa (Congreso de la República del Perú, 2013, p. 4).

Por su lado, en Costa Rica encontramos este delito con una designación totalmente diferente, pero con la misma noción de proteger a los sistemas y a la información digital.

Dicha conducta esta tipifica en el Código Penal en el artículo 229 ter, el cual dice:

> **Artículo 229 ter. - Sabotaje Informático:** Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.
>
> La pena será de cuatro a ocho años de prisión cuando:
>
> a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones (Asamblea legislativa de la república de Costa Rica, 1970, p. 89).

El Artículo 229 ter del Código Penal de Costa Rica y el Artículo 232 del Código Orgánico Integral Penal de Ecuador abordan la protección de sistemas informáticos y la integridad de la información contenida en estos. Ambos artículos sancionan con penas de prisión a quienes destruyan, alteren, obstaculicen o modifiquen sin autorización el funcionamiento de sistemas informáticos o bases de datos. En el caso de Costa Rica, el Artículo 229 ter contempla una pena de tres a seis años, que se incrementa a cuatro a ocho años si la conducta provoca peligro colectivo, es realizada por un empleado con acceso privilegiado y si afecta sistemas públicos o impide el acceso a personas autorizadas mediante medios tecnológicos.

Por otro lado, el Artículo 232 del Ecuador establece una pena de tres a cinco años para actos similares, incrementándose a cinco a siete años si se afecta la prestación de servicios públicos o la seguridad ciudadana. Ambos artículos coinciden en sancionar conductas que dañan o interfieren con sistemas informáticos, pero difieren en las circunstancias agravantes y las penas específicas establecidas para cada situación.

Existe un delito en el Ecuador denominado delitos contra la información pública reservada legalmente que en este caso sería contra el Estado, porque esta conducta recae sobre información que es reservada legalmente por el país, la tipificación de este delito asegura la protección de la privacidad y el secreto de Estado. Esta infracción penal vendría a relacionarse con delitos que de igual manera los encontramos en el Código Orgánico Integral Penal como son la interceptación ilegal de datos y la revelación ilegal de base de datos, el ya mencionado delito esta descrito de la siguiente manera:

> **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 (Código Orgánico Integral Penal, 2014, p. 78).

El Artículo 233 del Código Orgánico Integral Penal del Ecuador aborda los delitos contra la información pública reservada legalmente, estableciendo sanciones específicas para la destrucción, inutilización y revelación no autorizada de información clasificada. Este artículo se enfoca en proteger la integridad y seguridad de la información que, por su naturaleza, debe mantenerse reservada para salvaguardar el interés público y la seguridad del Estado.

Primero, el artículo tipifica la conducta de destruir o inutilizar información clasificada como un delito grave, imponiendo una pena de prisión de cinco a siete años. Esta disposición subraya la importancia de preservar la confidencialidad de la información que ha sido legalmente clasificada, ya que su destrucción o inutilización puede comprometer seriamente la seguridad y el funcionamiento adecuado de las instituciones que dependen de ella.

En segundo lugar, el artículo sanciona a los servidores públicos que obtengan información clasificada utilizando medios electrónicos o informáticos sin la debida autorización. De darse este caso la pena privativa de libertad sería de tres a cinco años de prisión, reflejando la seriedad con la que se considera el acceso no autorizado a información reservada. Este aspecto del artículo busca evitar que personas en posiciones de confianza utilicen su acceso a sistemas y datos sensibles de manera indebida.

Finalmente, el artículo establece sanciones aún más severas para los servidores públicos que revelen esta información reservada que pueda comprometer gravemente la seguridad del

Estado. En tales casos, la pena es de siete a diez años de prisión, además de una inhabilitación para ejercer funciones públicas por seis meses, siempre y cuando no se configure otra infracción de más grave. Esta disposición enfatiza el riesgo elevado asociado a la divulgación de información que podría tener un impacto significativo en la seguridad nacional, subrayando la necesidad de una gestión rigurosa y responsable de la información clasificada.

En conjunto, el Artículo 233 del COIP proporciona un marco claro y robusto para la protección de la información pública reservada, estableciendo penalidades específicas y severas para prevenir y sancionar el manejo indebido de datos clasificados. La combinación de penas privativas de libertad y sanciones adicionales para los servidores públicos refleja el compromiso del sistema legal ecuatoriano con la integridad de la información que es crítica para el funcionamiento y la seguridad del Estado.

El sexto delito que encontramos en la sección de delitos informáticos dentro de la norma penal local, es uno que tiene que ver con la privacidad de las personas y de los derechos que estas tienen sobre los sistemas informáticos, este delito se denomina de la siguiente manera:

> **Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.**
>
> 1. La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años.
>
> 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años (Código Orgánico Integral Penal, 2014, p. 79).

Este artículo aborda la conducta de las personas que logran el acceso no consentido a sistemas informáticos, telemáticos o de telecomunicaciones, estableciendo sanciones específicas para quienes ingresen a estos sistemas sin autorización. Este artículo está diseñado para proteger la integridad y seguridad de las redes y sistemas tecnológicos frente a accesos indebidos y explotación ilícita.

En primer lugar, el artículo tipifica como delito el acceso no autorizado a un sistema informático, telemático o de telecomunicaciones, sancionando a quienes ingresen total o parcialmente a dichos sistemas en contra de la voluntad de quienes tienen legítimo derecho sobre ellos. La pena establecida para esta conducta es de tres a cinco años de prisión. Esta disposición resalta la importancia de respetar la propiedad y los derechos de acceso a sistemas tecnológicos, penalizando la intrusión no autorizada que puede poner en riesgo la integridad de la información y los recursos de los propietarios legítimos.

En segundo lugar, el artículo agrava la pena cuando el acceso no autorizado se utiliza para fines adicionales, tales como explotar ilegalmente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz, u ofrecer servicios que los sistemas proveen a terceros sin pagar a los proveedores legalmente autorizados. En estos casos, la pena sigue siendo de tres a cinco años de prisión, pero la mención de actividades específicas como la modificación de portales web o el desvío de tráfico de datos indica una preocupación adicional por el uso indebido que puede tener un impacto más amplio y disruptivo en el funcionamiento de los sistemas afectados.

Este artículo refleja un enfoque integral hacia la protección de los sistemas informáticos y de telecomunicaciones, abordando no solo el acceso no autorizado, sino también las acciones ilícitas que pueden derivarse de dicho acceso, implicando combatir el espionaje informático.

Al sancionar de manera específica las conductas de explotación y modificación no autorizadas, el articulado busca disuadir el uso indebido de sistemas tecnológicos y garantizar la protección de la propiedad digital y los servicios que estos sistemas proporcionan. La pena establecida para estas infracciones refuerza el compromiso del marco legal ecuatoriano con la seguridad cibernética y la integridad de los recursos tecnológicos.

Ahora en el contexto penal colombiano, existe la tipificación de un delito similar que trata de sancionar la misma conducta, este se denomina así:

> **Art. 269-A.- Acceso abusivo a un sistema informático.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2000, p. 130).

Prácticamente se puede decir que son exactamente iguales, a excepción por la denominación y por la incorporación de un numeral más en el ciberdelito descrito en el Ecuador, la tipificación de estas conductas pretende mitigar la violación del derecho a la privacidad e intimidad y proteger datos y a los usuarios de las TICS, además también se resguarda la seguridad de los equipos informáticos.

Estas conductas son muy similares, y las breves diferencias encontradas están en las penas con que se castiga este tipo de ciberdelitos.

La conducta general en el Ecuador tiene una pena privativa de libertad de tres a cinco años y existe una distinción en donde si al acceder ilegítimamente a estos, el actor o sujeto activo quiere sacar provecho de esto, de igual manera se aplica la misma pena antes descrita.

En Colombia las penas restrictivas de la libertad son un poco más severas puesto que van de 4 a 8 años, además a esta se le agrega una multa que puede ir desde 100 a 1000 salarios mínimos legales mensuales vigentes.

En Perú de igual forma se encuentra tipificado este tipo penal y se nos explica de la siguiente manera:

> **Artículo 2. Acceso ilícito:** El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado (Congreso de la República del Perú, 2013, pp. 1-2).

Ambos artículos, uno del Congreso de la República del Perú y el otro del Código Orgánico Integral Penal de Ecuador, tratan sobre el acceso no autorizado a sistemas informáticos y presentan varias semejanzas y diferencias. En términos de semejanzas, ambos penalizan el acceso sin autorización a sistemas informáticos, en los dos casos este acceso puede ser total o parcial y en las dos legislaciones se lo sanciona con penas privativas de libertad.

En cuanto a las diferencias, el artículo peruano menciona específicamente la "vulneración de medidas de seguridad establecidas para impedirlo", mientras que el ecuatoriano no lo detalla en su primer párrafo. El artículo peruano también sanciona a quien accede "excediendo lo autorizado", lo cual no se menciona explícitamente en el texto ecuatoriano. Además, el artículo ecuatoriano detalla sanciones específicas para aquellos que accedan a sistemas con el propósito

de explotar ilegítimamente el acceso, modificar portales web, desviar o redireccionar tráfico de datos o voz, u ofrecer servicios sin pagar a los proveedores genuinos, una distinción que no se encuentra en el artículo peruano. Por último, el articulado del vecino país condena estas acciones con penas privativas de la libertad de 1 a 4 años, además se le agrega pena de treinta a noventa días multa. Por su parte Ecuador, castiga este delito con una pena restrictiva de la libertad de 3 a 5 años.

En resumen, ambos artículos abordan el acceso no autorizado a sistemas informáticos con penas de privación de libertad, pero difieren en aspectos como la vulneración de medidas de seguridad, las sanciones para exceder lo autorizado, los propósitos específicos del acceso ilícito, y la duración de las penas.

En Costa Rica no existe un delito denominado como tal, sin embargo, existe un tipo penal denominado Daño Informático:

> **Artículo 229 bis. - Daño Informático.** Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.
>
> La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable (Asamblea legislativa de la república de Costa Rica, 1970, p. 88).

Aquí se describe tácitamente alguna conducta similar a la de acceso no consentido a un sistema informático, la diferencia radica en que en Costa Rica incluye que además del ingreso sin autorización al sistema informático o se excede la autorización dada, se comete daño ante la información que se contiene en estos sistemas informáticos, también existe diferencia en las penas restrictivas de la libertad, mientras que en Ecuador son de tres a cinco años en Costa Rica son de uno a tres, ambos ciberdelitos tienen un inciso más, en Ecuador además se tipifica la explotación ilegítima de este sistema informático con la misma pena y en Costa Rica se agrava la pena si la información dañada no se puede recuperar y la pena aumenta de tres a seis años.

Como ultimo delito informático, descrito en esta sección del Código Orgánico Integral Penal, el legislador toma en cuenta la falsificación informática y la describe así:

> **Art. 234.1.- Falsificación informática:**

> 1. La persona que, con intención de provocar un engaño en las relaciones jurídicas, introducir, modificar, eliminar o suprimir contenido digital, o interferir de cualquier otra forma en el tratamiento informático de datos, produzca datos o documentos no genuinos, será sancionada con pena privativa de libertad de tres a cinco años.
>
> 2. Quien, actuando con intención de causar un perjuicio a otro o de obtener un beneficio ilegitimo para sí o para un tercero, use un documento producido a partir de contenido digital que sea objeto de los actos referidos en el número 1, será sancionado con la misma pena (Código Orgánico Integral Penal, 2014, p. 80).

El artículo 234.1 del Código Orgánico Integral Penal de Ecuador define el delito de falsificación informática. Este delito se caracteriza por dos acciones principales: la primera es la creación de datos o documentos no genuinos mediante la introducción, modificación, eliminación, supresión de contenido digital o interferencia en el tratamiento informático de datos con la intención de provocar un engaño en relaciones jurídicas. La sanción para esta acción es una pena privativa de libertad de tres a cinco años. La segunda acción sancionada es el uso de un documento producido a partir de dicho contenido digital falsificado, con la intención de causar un perjuicio a otro o de obtener un beneficio ilegítimo para sí o para un tercero. La pena para esta acción es la misma, de tres a cinco años de privación de libertad. Este artículo resalta la gravedad de manipular digitalmente la información con fines fraudulentos y la utilización posterior de dicha información falsificada para obtener ventajas indebidas o causar daños.

En Colombia, Perú y Costa Rica no se encuentra ningún artículo que describa este delito.

Analizando la legislación extranjera, específicamente en Costa Rica encontramos dos delitos en específico que no son considerados como tales en nuestro país, estos tipos penales son conductas que en el Ecuador se dan a diario y por su ausencia en la ley, quedan en la impunidad. Estos delitos son la Estafa Informática que en el Código Penal Costarricense se describe así:

> **Artículo 217 bis. - Estafa informática**. Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

> La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos (Asamblea legislativa de la república de Costa Rica, 1970, p. 84).

Y el otro delito se denomina Facilitación del delito informático, cuya tipificación se encuentra así:

> **Artículo 234.- Facilitación del delito informático**. Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos (Asamblea legislativa de la república de Costa Rica, 1970, p. 90).

En el contexto nacional, las estafas informáticas se dan a diario, los ciberdelincuentes se adaptan y cada vez buscan mejores maneras de lograr su cometido, surgen nuevos modos de estafa en donde las victimas creen el engaño y se les causa daño a su patrimonio, a respecto el diario El Universo nos menciona sobre los delitos informáticos más frecuentes en el país: “Los más frecuentes son las estafas digitales con modalidades como la suplantación de identidad y la apropiación fraudulenta a través de medios electrónicos (El Universo, 2020, p. 1).

Partiendo del concepto de estafa: “Apoderamiento de lo ajeno con aparente consentimiento del dueño, sorprendido en su buena fe o superado en su malicia” (Cabanellas, 2005), se deduce que la estafa es cuando una persona se adueña de algo que no es suyo, mediante algún artificio o trampa y engaño en contra del verdadero dueño, el cual, pensando que actúa correctamente le cede este bien al estafador. Dentro del Ecuador la estafa se encuentra descrita en el artículo 186 del Código Orgánico Integral Penal de la siguiente forma:

> La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años (Código Orgánico Integral Penal, 2014, p. 62).

Analizando este concepto se concluye que de igual manera se relaciona con el concepto de Cabanellas de Torres en donde se resalta que la similitud tácita se encuentra en que la persona

estafada, erróneamente perjudica su patrimonio porque ha sido engañado, se le ha mentido y timado, y el actúa con su propio consentimiento pensando que lo que realiza y lo que se le muestra es verdadero.

Con relación a los delitos informáticos, se sabe que se realizan estafas por estos medios, es la nueva modalidad hoy en día de atentar en contra del patrimonio de las personas, ejemplo de esto es que suplantan la identidad de una persona ya sea natural o jurídica y actúan de mala intención, existe el caso de que los delincuentes toman el nombre de una tienda y mediante medios electrónicos publican que comercializan los mismos artículos que la tienda original, a veces cambian la dirección del local y otras veces no, las víctimas se comunican con estos, de igual manera mediante sistemas informáticos, en este caso celulares o computadoras, y los estafadores los engañan diciendo que primero se les transfiera el dinero por la compra y luego se realizará él envió de la mercadería, la victima cree que es verdad y transfiere su dinero, los estafadores viendo esto bloquean a la víctima, la cual muchas de las veces no sabe ni quien fue el que los estafó. Otras veces mediante llamada telefónica se hacen pasar por familiares de las victimas engañándolos así para que se les transfiera dinero.

Este delito debería ser tomado en cuenta dentro de nuestra legislación puesto que no existe regulación jurídica al respecto, ya que el tipo penal tipificado en el Ecuador no aclara que se pueda realizar la estafa mediante medios electrónicos. Según la policía de ciberdelitos del país en cuanto a las estafas informáticas se nos precisa que: “En segundo lugar están las estafas en línea con 212 en 2021; 107 en 2022; y 67 en 2023” (Machado, 2024, p. 1), esto nos deja claro que esto se lleva a cabo con frecuencia, además que muchas de las ocasiones no se denuncia o al llegar a fiscalía se archiva el caso porque al momento de denunciar se lo hace con el delito de estafa, pero este no cubre lo que vendría siendo esta acción.

De esta manera se puede afirmar que la estafa informática es cuando una persona para obtener un beneficio patrimonial mediante engaño, simulación de hechos u ocultamiento de la verdad, induzca a error a otra con el fin de que realice un acto que perjudique su patrimonio, todo esto por medio de las TIC.

Por su parte la facilitación del delito informático sanciona a quien facilita el acceso a dispositivos listos para el cometimiento de cualquier delito informático. Es indispensable sancionar a la persona que ofrezca o publicite el cometimiento de estos delitos, puesto que esta conducta es considerada como dañina a la sociedad porque de igual forma es una acción que va

en contra de los derechos de las personas, en este caso en contra de todos los derechos que se violan en los delitos informáticos.

4.12. La Criminalidad

Partiendo de un concepto por parte del jurista Cabanellas de Torres la criminalidad es: "También, volumen total de infracciones o proporción en que se registran los crímenes en general, y las varias clases de crímenes en particular, en una sociedad o región determinada y durante cierto espacio de tiempo" (Cabanellas, 2005, p. 99), la definición de criminalidad proporcionada por Torres subraya la importancia de analizar tanto el volumen total de infracciones como la proporción en la que se registran diferentes tipos de delitos dentro de una sociedad o región específica durante un período determinado. Este enfoque es fundamental para comprender la magnitud y la distribución de la criminalidad, lo cual tiene varias implicaciones clave. En primer lugar, al considerar el volumen total de infracciones, se obtiene una visión general de la carga delictiva que enfrenta una sociedad, evaluando la magnitud del problema y planificando respuestas adecuadas. El análisis proporcional, por su parte, permite identificar qué tipos de delitos son más prevalentes, entendiendo las dinámicas específicas de la criminalidad y focalizando los esfuerzos de prevención y control en las áreas más críticas.

Además, evaluar la criminalidad en una región determinada y durante un espacio de tiempo específico ayuda a identificar patrones geográficos y temporales, detectando zonas con altas tasas de criminalidad o períodos del año en los que ciertos delitos aumentan, lo cual es esencial para la planificación de estrategias de seguridad pública. Por último, reconocer las varias clases de crímenes en particular permite descomponer la criminalidad en categorías específicas, como delitos contra la propiedad, delitos violentos o delitos cibernéticos, y diseñar intervenciones específicas que aborden las características únicas de cada tipo de delito. En resumen, el concepto de criminalidad según Torres aboga por un análisis integral y detallado que considere no solo la cantidad total de delitos, sino también su distribución y características específicas en un contexto dado, proporcionando una base sólida para el desarrollo de políticas públicas eficaces y estrategias de prevención del delito que sean informadas, focalizadas y adaptadas a las realidades específicas de la criminalidad en cada sociedad.

Siguiendo en esta línea la doctrina se asemeja mucho a este concepto, este se refleja en la siguiente referencia:

> Se puede definir a la criminalidad de muchas maneras, sin embargo, se la podría puntualizar como el conjunto de acciones que son realizadas por ciertos de individuos,

> que vulneran las leyes impuestas en sociedad, poniendo a la vista como resultado de ello el cometimiento de delitos, los mismos que generan daño e impacto social, a pesar de ello, es importante considerar las circunstancias en las que un individuo se convierte en “criminal o delincuente”, además de analizar la cantidad de transgresiones a la ley que se cometen en ciertos sectores y que de alguna manera pueden influir en el cometimiento de los delitos (Castillo, 2022, p. 16).

La definición de criminalidad que nos da Castillo es particularmente significativa porque ofrece una comprensión exhaustiva y multidimensional del fenómeno delictivo. Se puede desglosar en varios componentes clave que destacan la complejidad y las ramificaciones de los actos criminales. La criminalidad se percibe no solo como un conjunto de acciones ilegales, sino como conductas que, al infringir las leyes establecidas por la sociedad, resultan en delitos que tienen repercusiones profundas y variadas en la comunidad.

Uno de los aspectos cruciales que resalta esta definición es la necesidad de considerar las circunstancias específicas en las que un individuo se convierte en un "criminal o delincuente". Esta perspectiva invita a un análisis detallado de los factores personales, sociales, económicos y ambientales que pueden influir en la conducta delictiva. Por ejemplo, la pobreza, la falta de acceso a una educación de calidad, el desempleo y la exclusión social son factores que frecuentemente se correlacionan con mayores tasas de criminalidad. Al entender estos factores, se pueden diseñar intervenciones más efectivas y dirigidas a las raíces del problema en lugar de solo abordar sus síntomas.

Además, Castillo sugiere que el análisis de la cantidad de transgresiones legales en ciertos sectores puede ofrecer una visión más amplia del contexto en el que ocurren los delitos. La distribución geográfica y sectorial de la criminalidad puede revelar patrones que son críticos para la formulación de políticas de prevención y control del delito. Por ejemplo, las áreas con alta densidad de población y menos recursos tienden a mostrar mayores índices de criminalidad, lo que puede guiar la asignación de recursos y esfuerzos preventivos.

Esta definición también reconoce el impacto social de la criminalidad, destacando que los delitos no solo afectan a las víctimas directas sino también a la cohesión y el bienestar general de la comunidad. El miedo al delito puede alterar la vida cotidiana, restringiendo las actividades y deteriorando la confianza en las instituciones públicas. Por lo tanto, abordar la criminalidad requiere una estrategia holística que incluya no solo la aplicación de la ley sino también la mejora de las condiciones sociales y económicas que pueden prevenir la conducta delictiva.

En resumen, la definición de criminalidad de Castillo subraya la importancia de un enfoque integral para entender y combatir el delito. Al considerar tanto las acciones que constituyen delitos como las circunstancias contextuales y los factores sociales que los fomentan, se puede desarrollar una respuesta más efectiva y sostenible a la criminalidad. Esta perspectiva no solo busca reducir la incidencia delictiva, sino también fortalecer la cohesión social y mejorar la calidad de vida en la sociedad en general.

Desde un enfoque en donde la criminalidad es el volumen del conjunto de las conductas criminales, en relación a los delitos informáticos, podríamos dar como un ejemplo lo que nos cita el universo: "Los delitos informáticos van en aumento en Ecuador, según las denuncias presentadas en la Fiscalía, desde antes de la pandemia del COVID-19. En el 2017 se registraron 8421 casos; subieron a 9571 y 10279 en 2018 y 2019. La tendencia se mantiene (El Universo, 2020, p. 1), la criminalidad informática vendría siendo el conjunto de delitos informáticos que hoy en día se cometen en el Ecuador, dentro de estas actividades ilícitas podemos encontrar, la interceptación ilegal de datos, la apropiación fraudulenta por medios electrónicos, acceso no consentido a un sistema informático, estafas informáticas, entre otras.

4.13. La Ciberdelincuencia

La ciberdelincuencia es definida por la Real Academia Española como: "Actividad delictiva que se lleva a cabo a través de internet" (Real Academia Española, 2023, p. 1), esta definición subraya la naturaleza digital de los delitos informáticos, los cuales pueden variar desde la interceptación ilegal de datos, estafas informáticas, espionaje y el fraude cibernético. La creciente dependencia de la tecnología y la interconexión global ha facilitado la proliferación de estas actividades delictivas, afectando tanto a individuos como a organizaciones y estados.

Es fundamental que los marcos legales evolucionen para abordar eficazmente la ciberdelincuencia. Esto implica no solo la actualización de leyes y regulaciones, sino también el fortalecimiento de la cooperación internacional y el desarrollo de capacidades técnicas y humanas para la prevención, detección, y persecución de estos delitos. En este contexto, la formación de profesionales del derecho especializados en ciberseguridad y el derecho informático se convierte en una prioridad para enfrentar los retos que plantea este tipo de delincuencia.

La ciberdelincuencia abarca una amplia gama de actividades dañinas que se realizan a través del internet, estas son realizadas a través de la explotación de las tecnologías de la información y la comunicación.

La Oficina de las Naciones Unidas contra la Droga y el Delito nos dice que no existe una definición universal para lo que sería la ciberdelincuencia, más sin embargo nos expresa lo siguiente: “La ciberdelincuencia es un concepto complejo que engloba una variedad de actividades ilícitas que tienen como blanco las TIC o que las utilizan para cometer los delitos” (Oficina de las Naciones Unidas contra la Droga y el Delito, 2022, p. 8), esta perspectiva subraya la multifacética naturaleza de la ciberdelincuencia y la dificultad de encapsularla en una definición única y sencilla.

La UNDOC destaca dos aspectos clave de la ciberdelincuencia, primero, los delitos que tienen como objetivo directo las TIC, como los ataques a la infraestructura de red, el hacking y la distribución de malware; y segundo, los delitos tradicionales que se facilitan mediante el uso de TIC, como la estafa informática, el fraude electrónico y la pornografía infantil a través de internet. Esta dualidad refleja la versatilidad y la adaptabilidad de los ciberdelincuentes en la explotación de las tecnologías emergentes para sus fines ilícitos.

La falta de una definición universal complica los esfuerzos para combatir la ciberdelincuencia a nivel global, ya que las jurisdicciones nacionales pueden tener enfoques y legislaciones diferentes. Por lo tanto, es crucial fomentar la cooperación internacional y la armonización de las leyes para enfrentar eficazmente estos desafíos. Además, la complejidad inherente de la ciberdelincuencia exige un enfoque interdisciplinario, involucrando no solo a los profesionales del derecho, sino también a expertos en tecnología y seguridad cibernética, para desarrollar estrategias integrales de prevención y respuesta.

Con todo lo explicado anteriormente, se afirma entonces que la ciberdelincuencia es todo acto ilícito que se comete a través de medios informáticos o que tiene como fin el daño a estos.

4.14. Seguridad Jurídica

Partiendo nuevamente con un concepto del Diccionario de la Real Academia Española, se nos explica que la seguridad jurídica es: “Cualidad del ordenamiento jurídico que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación” (Real Academia Española, 2023, p. 1).

Esta definición subraya dos aspectos fundamentales como la certeza normativa y la previsibilidad en la aplicación de las normas jurídicas. La certeza normativa se refiere a la claridad, estabilidad y coherencia del marco legal, lo cual permite a los individuos y entidades conocer sus derechos y obligaciones con precisión. Por otro lado, la previsibilidad en la

aplicación de las normas asegura que los actos y decisiones legales se realizarán de manera consistente y conforme a la ley, reduciendo así la desigualdad y la incertidumbre.

La seguridad jurídica es esencial para el buen funcionamiento del Estado de derecho, ya que fomenta la confianza de los ciudadanos en el sistema legal y en las instituciones que lo administran. Sin esta seguridad, las personas y las empresas enfrentarían un entorno de incertidumbre y riesgo, lo que dificultaría la planificación y el desarrollo de actividades económicas y sociales. Además, la seguridad jurídica es un pilar fundamental para la protección de los derechos humanos y las libertades individuales, ya que garantiza que estos derechos sean reconocidos y respetados de manera uniforme y no sujeta a interpretaciones arbitrarias.

La importancia de la seguridad jurídica también se manifiesta en el ámbito internacional, donde la confianza en la aplicación predecible y justa de las normas jurídicas es crucial para las relaciones comerciales y diplomáticas entre los estados. En este contexto, la adopción de estándares legales internacionales y la cooperación jurídica entre países contribuyen a fortalecer la seguridad jurídica a nivel global.

En Ecuador la seguridad jurídica es un derecho fundamental consagrado en la Constitución de la República específicamente en el artículo 82 de la siguiente manera: “El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes” (Constitución de la República del Ecuador, 2008, p. 33). Esta disposición subraya la importancia de varios principios esenciales que conforman el núcleo de la seguridad jurídica: la supremacía constitucional, la previsibilidad normativa y la competencia de las autoridades.

El respeto a la Constitución implica que todas las normas y actos de las autoridades deben alinearse con los principios y disposiciones constitucionales, garantizando así un marco legal coherente y estable. La existencia de normas jurídicas previas y claras asegura que los ciudadanos y entidades puedan conocer con antelación las reglas que rigen su conducta, lo que permite una planificación adecuada y evita la arbitrariedad. La publicidad de las normas garantiza que estas sean accesibles para todos, promoviendo la transparencia y el conocimiento del derecho. Finalmente, la aplicación de las normas por autoridades competentes asegura que las decisiones legales sean tomadas por aquellos debidamente facultados y capacitados, de igual forma estas decisiones deben acogerse a lo estipulado por la ley, todo esto fortalece la confianza en el sistema de justicia.

La seguridad jurídica en Ecuador, como derecho constitucional, es fundamental para la protección de los derechos y libertades de los ciudadanos. Además, es un pilar esencial para el desarrollo económico y social del país, ya que proporciona un entorno de certeza y confianza necesario para las inversiones y las actividades comerciales. La previsibilidad y la claridad en la aplicación de las normas jurídicas reducen el riesgo de conflictos y litigios, facilitando así un ambiente de estabilidad y desarrollo sostenible.

Respetando la seguridad jurídica en el ámbito de los ciberdelitos, el Ecuador tipifica varias conductas ilícitas a través de medios informáticos dentro del Código Orgánico Integral Penal, sin embargo, respetando este derecho es fundamental aclarar y agregar más conductas de este tipo como lo es la estafa informática y la facilitación de delito informático, para así honrar este derecho primordial y que las personas puedan entender la ilicitud de sus conductas antes de cometerlas y de la misma forma los jueces y aplicadores de justicia del país puedan fundamentarse en la ley para sancionar este tipo de delitos.

5. Metodología

En el transcurso de esta investigación se emplearon diversos métodos, procedimientos y técnicas, que permitieron recabar información necesaria, relevante y de gran importancia para su desarrollo. Estos enfoques facilitaron una comprensión profunda y sistematizada de la problemática social planteada, lo que a su vez permitió el análisis exhaustivo y la propuesta de posibles soluciones.

5.1. Materiales utilizados

Durante el desarrollo del presente Trabajo de Integración Curricular, fue fundamental reconocer los materiales utilizados que permitieron alcanzar los objetivos propuestos. Entre estos materiales se incluyen libros, diccionarios jurídicos, manuales, revistas científicas, artículos científicos, y leyes. Especial mención merecen los sitios web de diversas instituciones judiciales, tanto a nivel internacional como local, los cuales han sido referenciados de manera organizada junto con sus respectivas fuentes bibliográficas.

Además de los materiales mencionados, también se utilizaron otros recursos complementarios para el desarrollo del trabajo, tales como un cuaderno de apuntes, teléfono celular, computadora, impresora y conexión a internet.

5.2. Métodos

En la presente investigación se harán uso de los siguientes métodos:

Método Inductivo: Es aquel que deriva conclusiones generales a partir de premisas individuales. En este contexto, busqué datos detallados para comprender el origen y el desarrollo de los delitos informáticos, así como su potencial impacto en la vulnerabilidad de los derechos de la ciudadanía.

Método Deductivo: El método deductivo implica partir de principios generales para llegar a conclusiones específicas. En este caso, lo apliqué en mi investigación para analizar y comparar delitos tipificados en Colombia, Perú y Costa Rica.

Método Hermenéutico: El método hermenéutico, en el ámbito de la investigación, tiene como objetivo adentrarse en el contenido de manera profunda, identificando y estructurando los elementos encontrados a lo largo del estudio. En mi investigación, usé este método en el Marco Teórico, donde analicé y contextualicé leyes, doctrinas y otros aspectos relevantes relacionados con la importancia del derecho informático.

Método Comparativo: En este trabajo de investigación, apliqué el método comparativo para analizar el Derecho Comparado, contrastando la realidad jurídica de Ecuador con el Código Penal de Colombia, Perú y Costa Rica.

5.3. Técnicas

Para la ejecución del presente Trabajo de Integración Curricular se emplearon las siguientes técnicas:

Técnicas de acopio teórico documental: Permitió la realización del marco teórico para un mejor aporte y desarrollo del trabajo mediante información actualizada y verídica, por medio de la selección de información de datos bibliográficos y documentales.

Técnicas de acopio empírico: Se conocen como técnicas de campo:

- **Encuesta:** Para aplicar esta técnica, se llevó a cabo un formulario de encuestas con preguntas claras y concretas, dirigidas a 30 profesionales del derecho, especialistas en informática y conocedores del problema, con el fin de obtener respuestas y recolectar datos. Una vez tabulados, se pudo conocer la opinión pública sobre la problemática planteada.
- **Entrevista:** Esta técnica se basó en la realización de preguntas con la ayuda de un formulario de entrevistas y equipo celular para la grabación, fue realizada a 5 profesionales del derecho, especialistas en informática y conocedores del problema, quienes respondieron acerca de aspectos concretos del tema de investigación, y sus respuestas fueron fundamentales para la obtención de información relevante acerca de la problemática planteada.

6. Resultados

6.1. Resultados de las Encuestas

En este apartado se pretender representar los resultados obtenidos durante la ejecución del trabajo de campo, las encuestas están conformadas por cinco preguntas y fueron aplicadas a 30 profesionales del derecho, especialistas en informática y conocedores del problema, mismas que arrojaron los siguientes resultados que a continuación son presentados.

Primera Pregunta

En otras legislaciones a diferencia de Ecuador se tipifica y sanciona así: en la Legislación Penal de Costa Rica la estafa informática y facilitación del delito informático. ¿Estima usted que la tipificación y sanción como delitos independientes de estas conductas en el Código Orgánico Integral Penal evitarían la impunidad?

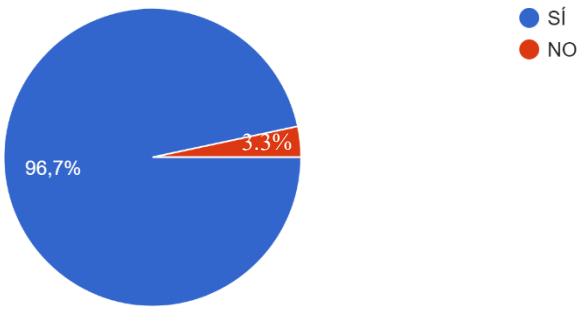
Tabla Nro. 1.

Indicador	Variables	Porcentaje
Sí	29	96.7%
No	1	3.3%
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autor: Gabriel Alejandro Cabrera Vivar

Figura Nro. 1.



Interpretación

En la presente pregunta se obtuvo los siguientes resultados, 29 de los 30 encuestados, que corresponden al 96,7% indicaron que la tipificación y sanción de la estafa informática y la

facilitación del delito informático como delitos independientes en el Código Orgánico Integral Penal si evitarían la impunidad de estas conductas; y por otro lado, 1 de los encuestados que representan el 3.3% indican que la tipificación y sanción de la estafa informática y la facilitación del delito informático como delitos independientes en el Código Orgánico Integral Penal no evitarían la impunidad de estas conductas.

Análisis

En la presente pregunta casi la totalidad de los encuestados, indicaron que la tipificación y sanción de la estafa informática y facilitación de delito informático como delitos independientes en el Código Orgánico Integral Penal si evitaría la impunidad de estas conductas. Respuesta con la cual comparto criterio, pues desde mi punto de vista, efectivamente al estar tipificadas estas conductas dentro de la norma penal del país, se tendría fundamento legal para perseguir y juzgar estas acciones ilícitas que dañan a la sociedad y que por no estar tomadas en cuenta dentro de los delitos informáticos del Ecuador se quedan en la impunidad.

Segunda Pregunta:

Considera usted que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delitos independientes:

Tabla Nro. 2.

Indicadores	Variables	Porcentaje
Estafa Informática	17	56.7%
Facilitación del delito informático	13	43.4%
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja

Autor: Gabriel Alejandro Cabrera Vivar

Figura Nro. 2.

Interpretación:

En la presente pregunta se obtuvieron los siguientes resultados, 17 de los 30 encuestados, que corresponden al 56.7% manifestaron que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delito independiente la estafa informática. Estos encuestados resaltan que este delito es el más cometido por medio de sistemas de información engañando a las personas para que cometan un error y puedan atentar contra su propio patrimonio por ende es al que más expuestos se encuentran las personas. Por otra parte, 13 de los encuestados que representan el 43.4% señalan que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delito independiente la facilitación del delito informático, ellos aseguran que se debe sancionar y castigar a aquellas personas que facilitan los medios electrónicos para cometer estos delitos informáticos, así realmente se garantizaría el ejercicio pleno de los derechos de la ciudadanía ecuatoriana, reforzando leyes que no los desamparen y los ayuden a buscar justicia.

Análisis:

Con respecto a esta pregunta, yo estoy totalmente de acuerdo con la opinión de la mayoría de los profesionales encuestados, que consideran que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delito independiente la estafa informática, porque de esta manera se

sancionaría esta conducta dañina, evitando en muchos casos el cometimiento de estas actividades, también se les da fundamento legal a las personas encargadas de administrar justicia como jueces, fiscales e incluso a la policía nacional para que puedan perseguir y combatir estos crímenes que van creciendo de manera acelerada día tras día. De esta forma se garantiza el pleno goce de los derechos de las personas ecuatorianas al tener fundamentos en la ley para poder disfrutar de un ciberespacio más sociable.

Tercera Pregunta:

¿Está usted de acuerdo en Reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación penal extranjera constituyen delitos informáticos?

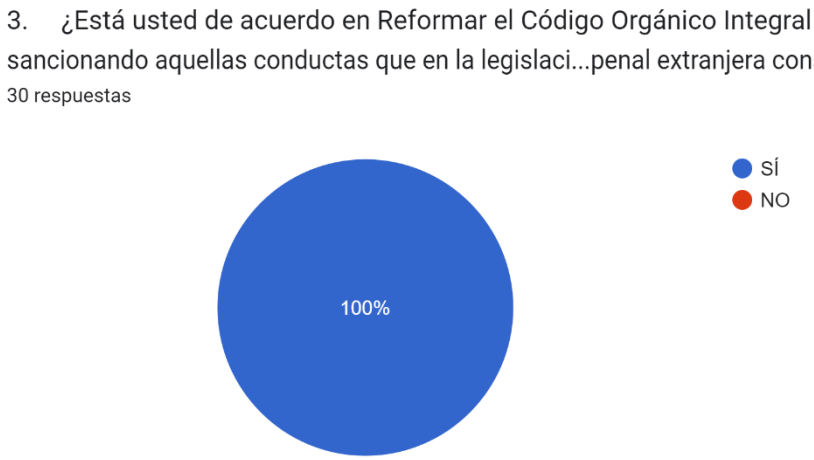
Tabla Nro. 3.

Indicadores	Variables	Porcentaje
Sí	30	100%
No	0	0%
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja

Autor: Gabriel Alejandro Cabrera Vivar

Figura Nro. 3.



Interpretación:

En la presente pregunta, 30 de los encuestados que corresponden al 100% afirmaron que están de acuerdo en reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación penal extranjera constituyen delitos informáticos, se puede apreciar una totalidad afirmativa, lo que nos indica que se mantiene una gran preocupación porque el legislador no toma en cuenta conductas que afectan a la sociedad, vulnerándoles sus derechos.

Análisis:

En la presente pregunta comparto la opinión de la totalidad de los encuestados, los cuales nos manifestaron que se encuentran de acuerdo con reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación penal extranjera constituyen delitos informáticos. Este resultado pone de manifiesto una preocupación generalizada sobre la capacidad que tiene el estado hoy en día para proteger los derechos de la sociedad en contexto a los delitos informáticos. Estas conductas son de las que más se realizan en el país y como no hay regulación jurídica al respecto los ciberdelincuentes operan con total tranquilidad. Reformando el COIP tendríamos mayor fuerza legal para la lucha contra la criminalidad informática.

Cuarta Pregunta:

¿Considera usted que tipificando y sancionando las conductas descritas anteriormente se disminuiría el índice de la delincuencia que delinque utilizando medios informáticos?

Tabla Nro. 4.

Indicadores	Variables	Porcentaje
Sí	29	96.7%
No	1	3.3%
Total	30	100%

Fuente: Profesionales del Derecho y especialistas en informática de la ciudad de Loja.

Autor: Gabriel Alejandro Cabrera Vivar

Figura Nro. 4.

Interpretación:

En la presente pregunta, 29 encuestados, que corresponden al 96.7%, indicaron de manera mayoritaria que tipificando y sancionando las conductas anteriormente descritas si se disminuiría el índice de la delincuencia que delinque utilizando medios informáticos. Considerando que los ciberdelincuentes se la pensarían dos veces al cometer estas conductas ya tipificadas. Por su lado, 1 encuestado, representando el 3.3%, manifestó que no disminuiría el índice de cometimiento de estas conductas por el solo hecho de tipificarlas y sancionarlas, esta discrepancia se fundamenta en que la reducción de la delincuencia responde a otro tipo de acciones como la política criminal.

Análisis:

Estoy totalmente de acuerdo con la mayoría de los resultados obtenidos en esta pregunta puesto que casi la totalidad de los encuestados sostiene que esta tipificación y sanción de conductas actuaría como un fuerte disuasivo contra los potenciales infractores y permitiría un procesamiento más efectivo de estos delitos, contribuyendo a una mejor seguridad y protección a la ciudadanía. Además de la disminución del índice de delitos informáticos se resalta entre los encuestados que gracias a la sanción de estos ilícitos se ayudaría a que los derechos violentados de las personas sean reparados y no se queden en la impunidad.

Quinta Pregunta:

¿Qué sugiere frente al problema planteado?

Interpretación

Dentro de esta pregunta los encuestados comparten varias opciones para hacer frente al problema planteado en donde se destaca por ejemplo, la tipificación de más delitos informáticos; establecer un mecanismo para revisar y actualizar las leyes relacionadas con delitos informáticos para adaptarse a las nuevas realidades de la ciberdelincuencia; auto informarse por parte de la ciudadanía acerca de los riesgos que todos corremos en la era de la información, puesto que muchas veces pensamos que el Estado puede hacerse cargo de todos los problemas que nos rodean y esto no siempre es así, pues el cuidado y la prevención, para algunos delitos, nos corresponden primero a nosotros como individuos; promover la cooperación internacional en la persecución e investigación de estos delitos; invertir en seguridad informática a través de la policía nacional y fiscalía para que de mejor manera puedan ganar la lucha contra estos delitos; campañas de concientización sobre la delincuencia informática; capacitación a la policía nacional, fiscalía y jueces en relación a delitos informáticos.

Análisis:

Estoy de acuerdo con muchas propuestas por parte de los encuestados con relación al problema planteado, pero con la noción con la que más apego encuentro en con la reforma legislativa del Código Orgánico Integral Penal para estudiar y agregar nuevas conductas por medios electrónicos, puesto que de esta manera, se puede perseguir estos delitos con el respaldo de la ley, evitando así que por vacíos legales estas acciones dañinas no sean perseguidas ni juzgadas, también estoy totalmente de acuerdo con promover la cooperación internacional, pues como se sabe los delitos informáticos no tienen barreras, algunas veces los actores se encuentran en otros estados lejos de donde se encuentra la víctima, con esta cooperación se lograría una mejor prevención y persecución entre estados de estos delitos, además del intercambio de información y capacitaciones que pueden fortalecer el conocimiento respecto de esta materia, y finalmente estoy de acuerdo en invertir fondos para las respectivas divisiones de la policía y fiscalía nacional, para que puedan tener los implementos y tecnología necesaria en la investigación de estos delitos y así asegurar que ninguno se quede impune.

6.2.Resultados de las entrevistas

Para avanzar en el desarrollo de las entrevistas, se formularon cinco preguntas abiertas dirigidas a cinco profesionales del derecho y especialistas en informática de la ciudad de Loja, quienes conocen a fondo el problema en cuestión. Estas entrevistas permitieron a los participantes

razonar y expresarse libremente, proporcionando valiosa información basada en su criterio y experiencia. Sus ideas innovadoras enriquecieron significativamente la investigación.

Este enfoque facilitó una óptima comprensión de la problemática planteada y la identificación de las falencias existentes. Las entrevistas se grabaron con un teléfono celular y se transcribieron para este documento, donde se realiza un análisis e interpretación detallada de sus respuestas.

Primera Pregunta:

En otras legislaciones a diferencia de Ecuador se tipifica y sanciona así: en el Código Penal de Costa Rica la estafa informática y la facilitación del delito informático. ¿Estima usted que la tipificación y sanción como delitos independientes de estas conductas en el Código Orgánico Integral Penal evitarían la impunidad?

Respuestas:

Primer entrevistado: Considero que el COIP necesita una reforma urgente en este tema de delitos cibernéticos porque Ecuador actualmente no cuenta con una normativa específica para este tipo de delitos tal como tú lo mencionas que es la estafa informática pues actualmente en Ecuador existe bastante pero como tal no pueden sancionarla porque no está tipificada, los jueces no tienen una normativa donde respaldarse y poder dar una pena al autor de este delito, quedando en la impunidad, así mismo la facilitación del delito informático, actualmente en el Ecuador se da bastante porque el facilitador es una persona que, te pongo un ejemplo dentro de una institución una persona que está filtrando la información, y como te mencionaba el facilitador vendría a ser un cómplice del delito, sucede esto bastante en el tema de bancos, en el tema de que se filtran bastantes números de tarjetas para poder embaucar y robar dinero a ciertas personas, pudientes obviamente, y bueno los delincuentes no miran realmente a las personas que roban, actualmente se han varias investigaciones y tengo conocimiento porque trabajo en una institución financiera sobre el cometimiento de estos delitos como tal el COIP no los sanciona ni los tipifica entonces los jueces llegan únicamente hasta un nivel de investigación previa como tal en fiscalía, los cuales no encuentran los elementos de convicción completos para poder pasar a una audiencia de juicio o un juicio final, considero que si se debería tipificar estos delitos en el COIP y hacer constar estos delitos para en cierta parte crecer en el ámbito judicial dentro del Ecuador y así evitar la impunidad.

Segundo entrevistado: Sí en este caso si evitarían bastante la impunidad ya que a nivel de Ecuador existen bastantes tipos de estafas que se dan a nivel informático, cabe recalcar que cada vez hay más medios para hacerlos, vía correo, WhatsApp, Facebook, esas vías son las más utilizadas en este caso no hay una sanción dura por decirlo de alguna manera a estos delitos, en este la fiscalía cuando se presenta este tipo de delitos no le toman mayor importancia y dejan que pase en su mayoría archivan estos casos, entonces si deberían haber esto en el COIP.

Tercer entrevistado: No, ya que son delitos que se pueden juzgar o acoplar con el tipo penal de delitos existentes.

Cuarto entrevistado: Es inevitable el avance tecnológico, el cual trae consigo muchas situaciones favorables. Sin embargo, también uno queda expuesto a los delitos informáticos por lo que considero que es fundamental que se incorporen herramientas legales para mitigar estos delitos.

Quinto entrevistado: Si, al encontrarse establecido en nuestro Código Orgánico Integral Penal, se puede normar las sanciones correspondientes para los delitos informáticos, en virtud de ello, se dejaría un precedente, el cual no dejaría en la impunidad referidos delitos, además de ser indispensable en el país para penar los delitos informáticos y evitar que se sigan cometiendo los mismos.

Comentario del Autor:

En base a la información proporcionada, se puede resumir que la mayoría de entrevistados están de acuerdo en que la tipificación de conductas que encontramos en la legislación extranjera evitaría la impunidad de estos hechos.

El primer entrevistado resalta que la ausencia de tipificación en el COIP resulta en que muchos casos no progresen más allá de una investigación preliminar, ya que no existen elementos legales claros para sancionar a los infractores. Esta carencia de normativa específica conlleva a la impunidad, lo cual es respaldado por la experiencia profesional del entrevistado en una institución financiera.

El segundo entrevistado concuerda en que la tipificación específica evitaría la impunidad y subraya que actualmente, la fiscalía no da la importancia debida a estos casos, lo cual resulta en archivos prematuros de muchos de ellos. Esto demuestra la urgencia de contar con un marco legal que permita una acción más efectiva y rigurosa por parte de las autoridades judiciales.

En contraposición, el tercer entrevistado opina que los delitos informáticos pueden ser juzgados bajo los tipos penales existentes, lo cual sugiere una percepción de suficiencia en la normativa actual. No obstante, esta perspectiva parece no considerar la particularidad y complejidad de los delitos cibernéticos que requieren un tratamiento especializado para ser efectivamente combatidos.

El cuarto entrevistado enfatiza la inevitabilidad del avance tecnológico y la exposición a nuevos tipos de delitos que este avance conlleva. La incorporación de herramientas legales específicas es fundamental para mitigar estos riesgos, reflejando una visión proactiva y adaptativa frente a los desafíos del mundo digital.

Finalmente, el quinto entrevistado considera que la inclusión de estos delitos en el COIP establecería un precedente crucial para la sanción de los delitos informáticos, marcando un paso indispensable para penar adecuadamente estas conductas y prevenir su proliferación. Este enfoque no solo aborda la necesidad de sanción, sino también el valor de establecer normas claras que actúen como disuasión. Podemos decir entonces que la tipificación y sanción específica de la estafa informática y la facilitación del delito informático en el COIP de Ecuador es esencial para cerrar las brechas legales actuales, fortalecer el marco judicial y evitar la impunidad. Esto permitiría a las autoridades actuar con mayor eficacia y rigor, garantizando así una respuesta adecuada a los desafíos que plantea el cibercrimen en nuestra sociedad.

Segunda pregunta:

¿Considera usted que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delitos independientes los siguientes: Estafa Informática, Facilitación del delito informático?

Respuestas

Primer entrevistado: Si, como te mencione a través de esta reforma del COIP agregar más delitos aparte de estafa informática y facilitación del delito, o sea son unos delitos conocidos a nivel mundial porque son los tipos de delito más común que están ocurriendo a nivel mundial, pero considero pues que si deberían tipificarse y sancionarse otros tipos de delitos, mas aun que se empezó a utilizar la realidad virtual, esta se puede usar para realizar varias cosas dentro del ciberespacio. Entonces si considero que se garantizaría el ejercicio pleno de los derechos de la ciudadanía ecuatoriana al tipificarse y sancionarse en el Código Orgánico Integral Penal los

delitos como la estafa informática y la facilitación del delito informático, pero además vuelvo a repetir se debería sancionar más delitos virtuales.

Segundo entrevistado: Si debería sancionarse porque a nivel de Ecuador existe bastantes tipos, uno de los casos más sonados que fue cuando vendieron datos de personas para realizar estafas en pirámides recién el Ecuador ahí quiso implementar una ley de protección de datos, pero a la final esta política no hace mayores, en si no sanciones serias para estas personas, solamente existe como una protección a los datos, pero a la final los delitos van a seguir impunes no va a haber una sanción grave a estas personas.

Tercer entrevistado: Sí, se aplicaría sanciones acordes al delito tecnológico y los juzgadores no tendrían que acoplarlos a otros tipos penales.
Cuarto entrevistado: Es necesario a efecto de garantizar el buen uso de nuestra información.

Quinto entrevistado: Si, para garantizar los derechos fundamentales de los ecuatorianos se debe normar la estafa informática y facilitación del delito informáticos de forma independiente; una vez tipificados los delitos antes referidos se tendría una herramienta de vanguardia para la sanción de los diversos delitos informáticos.

Comentario del autor:

El primer entrevistado subraya la necesidad no solo de incluir la estafa informática y la facilitación del delito informático, sino también de ampliar el espectro de delitos cibernéticos tipificados en el COIP. La realidad virtual y otras innovaciones tecnológicas han introducido nuevas formas de criminalidad que deben ser abordadas por la legislación para proteger eficazmente los derechos de los ciudadanos. Este enfoque integral es esencial para mantenerse a la par con el desarrollo tecnológico y sus implicaciones legales.

El segundo entrevistado destaca la falta de sanciones serias para los delitos informáticos actuales, citando ejemplos de casos notorios en los que la legislación ecuatoriana ha fallado en proporcionar una protección adecuada y sanciones proporcionales. La implementación de leyes de protección de datos, aunque un paso en la dirección correcta, no ha sido suficiente para prevenir y sancionar efectivamente estos delitos. Esto pone de relieve la necesidad de una normativa penal más robusta y específica.

El tercer entrevistado apoya la idea de sancionar estos delitos de manera acorde a su naturaleza tecnológica, evitando la necesidad de encajarlos en tipos penales tradicionales que no reflejan

adecuadamente la gravedad y particularidad de los delitos informáticos. Esto proporcionaría a los jueces una base legal más clara y adecuada para imponer sanciones justas y efectivas.

El cuarto entrevistado resalta la importancia de proteger la información personal de los ciudadanos, señalando que la tipificación de estos delitos es crucial para garantizar el buen uso de la información y prevenir abusos. En un mundo donde la información es un recurso valioso, la protección legal de los datos personales y la sanción de su uso indebido son esenciales para salvaguardar los derechos de los individuos.

Y, por último, el quinto entrevistado reafirma que, para garantizar los derechos fundamentales de los ecuatorianos, es imprescindible normar la estafa informática y la facilitación del delito informático de forma independiente. La tipificación de estos delitos proporcionaría una herramienta legal de vanguardia para la sanción de los diversos delitos informáticos, fortaleciendo así la capacidad del sistema judicial para abordar estas nuevas formas de criminalidad. Se deduce entonces que, la tipificación y sanción específica de la estafa informática y la facilitación del delito informático en el COIP es crucial para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana. Al abordar estas conductas de manera específica y proporcionada, se fortalecerá la protección legal de los ciudadanos, se mejorará la capacidad de las autoridades para sancionar efectivamente estos delitos y se contribuirá a la creación de un entorno digital más seguro y justo para todos.

Tercer Pregunta:

¿Está usted de acuerdo en Reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación extranjera constituyen delitos informáticos?

Respuestas:

Primer entrevistado: Sí totalmente de acuerdo

Segundo entrevistado: Si debería porque muchas de las veces no hay sanciones para estos delitos, si se debería reformarse el COIP para poder minimizarse esto.

Tercer entrevistado: Sí siempre y cuando no se afecte otros derechos de las personas.

Cuarto entrevistado: El delito informático es el acceso o el uso de nuestros datos sin el consentimiento en actividades o procesos ilícitos, estoy de acuerdo en reformar el COIP.

Quinto entrevistado: Si, actualmente nos encontramos en constante evolución de las Tecnologías de la Información y Comunicación, con ello, existe un progreso en las diversas maneras de delinquir, razón por la cual, la aplicación de alguna reforma al Código Integral Penal puede llegar a ser el medio idóneo para prevenir, vigilar y sancionar los delitos informáticos; protegiendo así derechos y garantías establecidas en nuestra Constitución.

Comentario del Autor:

El primer entrevistado muestra un apoyo total a la reforma del COIP, lo que refleja una comprensión clara de la urgencia y necesidad de adaptar la legislación ecuatoriana a los estándares internacionales en materia de delitos informáticos. Esta alineación con las normativas extranjeras no solo fortalecería la capacidad del país para combatir estos delitos, sino que también facilitaría la cooperación internacional en la persecución de delincuentes cibernéticos.

El segundo entrevistado enfatiza la falta de sanciones adecuadas para los delitos informáticos bajo la legislación actual. Señala que la reforma del COIP es esencial para minimizar la incidencia de estos delitos, lo cual es crucial para aumentar la eficacia del sistema judicial en la protección de los derechos de los ciudadanos frente a las amenazas cibernéticas.

El tercer entrevistado apoya la reforma siempre y cuando no se afecten otros derechos de las personas. Esta postura destaca la importancia de un equilibrio cuidadoso en la legislación, asegurando que las nuevas disposiciones no infrinjan los derechos fundamentales de los individuos mientras se combate eficazmente la criminalidad cibernética.

El cuarto entrevistado describe el delito informático como el acceso o uso no consentido de datos en actividades ilícitas y expresa su acuerdo en reformar el COIP, esto subraya la necesidad de proteger los datos personales de los ciudadanos, un componente esencial de la seguridad digital y la privacidad en la era moderna.

El quinto entrevistado refuerza la idea de que la evolución constante de las TIC implica nuevas formas de delinquir, lo que justifica plenamente la reforma del COIP. Menciona que dicha reforma es el medio idóneo para prevenir, vigilar y sancionar los delitos informáticos, asegurando así la protección de los derechos y garantías establecidos en la Constitución ecuatoriana. Es así que, reformar el COIP para incluir la tipificación y sanción de las conductas que en la legislación extranjera constituyen delitos informáticos es crucial para enfrentar eficazmente los desafíos del cibercrimen. Esta reforma permitiría al sistema judicial

ecuatoriano adaptarse a las nuevas realidades tecnológicas, protegiendo mejor a los ciudadanos y sus datos personales, y asegurando un entorno digital más seguro y equitativo. La unanimidad de los entrevistados en apoyar esta medida refuerza la necesidad de una acción legislativa inmediata y bien informada para fortalecer la lucha contra los delitos informáticos en Ecuador.

Cuarta pregunta:

¿Considera usted que tipificando y sancionando las conductas descritas anteriormente se disminuiría el índice de la delincuencia que delinque utilizando medios informáticos?

Respuestas

Primer entrevistado: Totalmente porque si nos ponemos a pensar que en estos delitos informáticos son personas que son retraídas de la sociedad, no son muy sociables, son personas de que al momento de que van a ver una tipificación o que existe una sanción para lo que están haciendo lo cual es un delito se van a cohibir de cometer estos actos, entonces considero pues que si se va a frenar demasiado los delitos informáticos con esto.

Segundo entrevistado: Sí minimizaría un gran porcentaje, incluyendo esto en el COIP si disminuiría bastante esto.

Tercer entrevistado: No, ya que esto solo buscaría una sanción más justa y el índice de delincuencia se debe más a temas sociales.

Cuarto entrevistado: Ayudaría a mitigar el problema, pero no lo desaparecería.

Quinto entrevistado: Es posible que el índice disminuya, en virtud de que actualmente no se encuentra normado algunos delitos informáticos, motivo por el cual, los delincuentes usan esta falencia a su favor para cometer dichos delitos; sin embargo, si existiera una norma legal sancionadora, permitiría precautelar derechos constitucionales y sería un instrumento fundamental para enfrentar de manera efectiva, tales conductas delictivas en el ámbito de las TIC.

Comentario del autor:

El primer entrevistado considera que la tipificación y sanción específica de los delitos informáticos disuadiría a muchos potenciales delincuentes. Este punto de vista se basa en la idea de que quienes cometen delitos informáticos suelen ser individuos con poca integración social, que se cohibirían ante la existencia de sanciones claras y específicas. Esto sugiere que

un marco legal robusto podría tener un efecto disuasorio significativo, frenando la comisión de estos delitos.

El segundo entrevistado coincide en que incluir estas conductas en el COIP disminuiría notablemente su incidencia. Este argumento refuerza la noción de que la certeza de una sanción específica y adecuada puede reducir la criminalidad, actuando no solo como un castigo, sino también como una prevención efectiva.

El tercer entrevistado, sin embargo, plantea que la tipificación y sanción de estos delitos no necesariamente disminuiría el índice de delincuencia, ya que este problema tiene raíces más profundas en temas sociales. Esta perspectiva destaca que, aunque las medidas legales son cruciales, deben ir acompañadas de políticas sociales y educativas que aborden las causas subyacentes de la delincuencia.

El cuarto entrevistado también es cauteloso al respecto, afirmando que, aunque la tipificación ayudaría a mitigar el problema, no lo eliminaría por completo. Esto sugiere que, si bien las sanciones legales son una parte esencial de la solución, no son suficientes por sí solas y deben integrarse en una estrategia más amplia que incluya medidas preventivas y de rehabilitación.

El quinto entrevistado es optimista sobre la posibilidad de que el índice de delincuencia disminuya con la tipificación de estos delitos. Argumenta que la actual falta de normativas específicas permite a los delincuentes explotar esta falencia. La existencia de una norma sancionadora específica no solo protegería los derechos constitucionales, sino que también proporcionaría una herramienta fundamental para enfrentar efectivamente las conductas delictivas en el ámbito de las TIC.

Quinta pregunta:

¿Qué sugiere frente al problema planteado?

Respuestas

Primer entrevistado: Como te mencione al inicio de la entrevista una reforma al COIP tipificando delitos a través de medios telemáticos obviamente abarcando varios tipos penales a través de medios telemáticos como te mencionaba un ejemplo más seria el acoso virtual como lo llamaron en Estados Unidos pero no se lo puede llamar aquí en la legislación ecuatoriana como tal este acoso virtual porque no existe, son términos nuevos, así mismo como va avanzando la humanidad va creciendo actualizándose cada vez más, también la delincuencia va actualizándose cada vez más, entonces si considero pues que ecuador en esta parte si se está

quedando un poquito la función judicial chapado a la antigua diciéndolo en el vocablo popular como se dice pero si debería actualizarse cada vez más, y lo que se debería hacer es una Reforma al COIP y actualizar esto.

Segundo entrevistado: Bueno mi sugerencia aquí seria que realmente se busque mediante la ley como una manera de como garantizar que la ciudadanía tenga un respaldo en caso de sufrir una estafa informática o cualquier otro delito informático ya que actualmente no hay sanción e incluso algo que se da es mucho la venta de información delicada por parte de las empresas de los clientes para hacer estas estafas y como sugerencia que al momento en el de legislar leyes siempre se busque cuáles son los mediadores en estos delitos, porque muchas veces no se puede encontrarlos ya que no son rastreables, que busquen la garantía de que se pueda identificar cual es el causante de esto. Buscar herramientas para garantizar la captura de estos ciberdelincuentes.

Tercer entrevistado: Implementar normas que permitan a cada uno de los magistrados administrar de mejor manera la justicia.

Cuarto entrevistado: Establecer herramientas legales para combatir el cibercrimen, una propuesta como ya dije seria reformar el COIP, conforme a la interrogante tercera.

Quinto entrevistado: Es de gran relevancia sugerir la revisión de las leyes existentes (estudio comparativo entre legislaciones) para la posible implementación de normativa que ayude a no dejar en la impunidad ningún delito informático, porque si bien es cierto el avance de las TICS se desarrolla día a día y asimismo los actos delictivos en las ellas.

Al realizar un minucioso análisis de la normativa legal vigente con respecto a los delitos informáticos, se encontraría vacíos legales existentes, con ello se debe plantear una reforma sancionadora al COIP, en la cual desarrolle, mejore e implemente sanciones a los actos ilícitos que se efectúan con la ayuda de las Tecnologías de la Información y Comunicación.

Comentario del Autor:

El primer entrevistado destaca la necesidad urgente de una reforma al Código Orgánico Integral Penal que tipifique y sancione los delitos cometidos a través de medios telemáticos. La actualización de la legislación para incluir términos y conductas emergentes, como el acoso virtual, es crucial para mantener la relevancia y efectividad de las normas penales. Este punto subraya la importancia de que el sistema judicial se mantenga al día con los avances tecnológicos y las nuevas formas de criminalidad.

El segundo entrevistado sugiere que la legislación debe garantizar respaldo a las víctimas de delitos informáticos y enfocarse en identificar y capturar a los ciberdelincuentes. Esto incluye la implementación de herramientas que permitan rastrear y localizar a los responsables de estos delitos, superando los desafíos técnicos que actualmente dificultan su identificación y enjuiciamiento.

El tercer entrevistado aboga por la implementación de normas que faciliten a los magistrados administrar la justicia de manera más eficaz. Esta noción vendría siendo más efectiva si se incluirían también capacitaciones para los jueces en materia de delitos informáticos.

El cuarto entrevistado reitera la necesidad de establecer herramientas legales específicas para combatir el cibercrimen, coincidiendo con la propuesta de reformar el COIP. Esta reforma debe estar orientada a abordar las particularidades de los delitos informáticos y proporcionar un marco legal claro y específico para su sanción.

El quinto entrevistado sugiere realizar un análisis comparativo de las legislaciones existentes en otros países para identificar y subsanar los vacíos legales en la normativa ecuatoriana. Este estudio permitiría implementar las mejores prácticas y adaptar las leyes nacionales a los estándares internacionales, garantizando así una protección más robusta contra los delitos informáticos. La reforma del COIP debe enfocarse en desarrollar, mejorar e implementar sanciones específicas para los actos ilícitos que se llevan a cabo utilizando las Tecnologías de la Información y Comunicación.

Se puede decir que, las sugerencias de los entrevistados convergen en la necesidad de una reforma integral del COIP que incluya la tipificación y sanción de los delitos informáticos, el desarrollo de herramientas para la identificación y captura de ciberdelincuentes, y la provisión de recursos y capacitación adecuados para el sistema judicial. Además, un análisis comparativo de legislaciones extranjeras puede proporcionar valiosas lecciones y estrategias para fortalecer la respuesta legal de Ecuador ante los desafíos del cibercrimen. Estas medidas combinadas serían fundamentales para reducir la impunidad y proteger los derechos de los ciudadanos en el entorno digital.

6.3. Estudio de casos

En la presente investigación se analiza el estudio de casos que se encuentran relacionados con la tipificación y sanción de la estafa informática y facilitación de delito informático. Es importante mencionar que, al ser un tema relativamente nuevo, no existen sentencias

ejecutoriadas, pero es preciso mencionar que basta con revisar los siguientes casos para respaldar la propuesta de reforma planteada.

6.3.1. Caso Nro. 1.

Datos referenciales

Juicio No. 17282-2018-01215

Juzgado: Tribunal de Garantías Penales de Pichincha

Procesados: Jorge Jairo Gavilanes Anchundia, Cinthia Mariela de la Torre Carriel, Byron Patricio Briones Rivas.

Actor: Fiscalía General del Estado

Delito: Art. 234 Acceso no consentido a un sistema informático, o de telecomunicaciones.

Fecha: 05/09/2018

Antecedentes

El presente proceso penal tiene como antecedente la instrucción fiscal iniciada por el DR. Alex Castillo Ardilla, Fiscal de la Provincia de Pichincha, en contra de los ciudadanos Jorge Jairo Gavilanez Anchundia y Cinthia Mariela de la Torre Carriel por el presunto delito de Acceso no consentido a un sistema informático, telemático o de telecomunicaciones tipificado y sancionado en el Art. 234 del COIP, luego se vinculó en la misma al ciudadano Byron Patricio Briones Rivas.

La Fiscalía llega a conocer la noticia criminis mediante denuncia presentada por la Dra. Silvia Lorena Villagómez Cabezas procuradora judicial de NAGRAVISION S.A., que en lo principal refiere lo siguiente: “Se desprende que mediante el sub dominio "http://iksprivadoecuador.all.ec/", el cual está ligado al dominio all.ec, se promociona “El servicio iks privado completo y efectivo", ofertando: "PLANES DE CALIDAD ECONÓMICA SERVER 95% Y FULL SERVER 100%", "los mejores canales latinos hd-sd- satélite amazonas". Esta oferta de televisión por suscripción (televisión paga) supone que quien la hace tiene el permiso correspondiente del órgano de control que le permite retransmitir contenidos exclusivos de televisión referentes a una plataforma multicanal; en este caso, la del Satélite Amazonas; y, además, cuenta con el contrato que le autoriza decodificar la señal y programación de dicho satélite. Quien realiza la promoción antes mencionada señala como

"contacto: WhatsApp0997689647 email:iksprivadoecuador@hotm.ail.com" info@iks61tv.com. Al realizar una búsqueda en la WEB referente la servidor "IKS61" se puede identificar qué el servicio de televisión paga antes mencionado se comercializa a través de los links http://www.iks61tv.com/,https://twitter.com/iks61, https://www.youtube.com/watch/IKSTV en los cuales aparecen como números de contacto telefónico, las siguientes líneas telefónicas: 00593-99128884.· y 0054-2616963068, la primera corresponde a telefonía celular del Ecuador, y la segunda aparentemente a telefonía celular de Argentina, lo cual lleva a colegir que la comercialización se realiza de forma local e internacional. Al tomar contacto a los números telefónicos mencionado, el posible consumidor recibe instrucciones del "servicio" prestado, se le explica que se trata de un "servicio alternativo" que será prestado con la reserva del caso, únicamente después de confirmar que los datos del cliente sean reales, adelantando que el pago por el "kit completo de FTA" y "el servicio de la señal" deben ser depositados en la cuenta bancaria de ahorros del banco del Pichincha No. 4112180300, Banco de Guayaquil cuenta de ahorros No. 37412460 y Banco del pacifico cuenta corriente No. 0741271…." Con estos hechos se da inicio a la investigación previa el 04 de enero del 2017 logrando establecer que los depósitos por el "supuesto servicio" se pide que deposite en varias cuentas de instituciones bancarias entre las que constaba la cuenta de ahorros del Banco del Pichincha No. 4112180300 cuya titular es la señora CINTHIA MARIELA DE LA TORRE CARRIEL. Fiscalía a través de la prueba de carácter pericial, testimonial y documental tiene como pretensión jurídica acreditar una conducta típica, antijuridica y culpable que se encuentra contemplado en el artículo 234 del Código Orgánico Integral Penal.

Resolución

Luego de haber realizado un examen crítico, mesurado y exhaustivo de la prueba presentada, de conformidad con las reglas de sana crítica y lógica jurídica, y el artículo 455 del COIP, y por cuanto se ha determinado el nexo causal entre la existencia de la infracción y la responsabilidad de los acusados en el cometimiento de dicha infracción, esto es, se ha determinado las categorías dogmáticas para que un acto u omisión pueda ser considerado delito, esto es, tipicidad, antijuridicidad y culpabilidad, al haberse desvirtuado la presunción de inocencia garantizada en el Art. 76.2 de la Constitución de la República, más allá de toda duda razonable, esta Autoridad, ADMINISTRANDO JUSTICIA, EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, debido a que se ha comprobado conforme a derecho que los acusados ha adecuado su conducta al delito de Acceso no consentido a un sistema informático, telemático o

de telecomunicaciones, tipificado y sancionado en el Art. 234 del COIP, en calidad de autores (Art. 42.1.a ibídem), declaro su culpabilidad y dicto SENTENCIA CONDENATORIA en contra de BYRON PATRICIO BRIONES RIVAS y JORGE JAIRO GAVILANEZ ANCHUNDIA, cuyas generales constan en el expediente, y les impongo la pena de UN AÑO DE PRISION a cada uno, que en el caso del ciudadano BYRON PATRICIO BRIONES RIVAS la deberá cumplir en uno de los centros de rehabilitación social de varones de la ciudad de Guayaquil, y el otro, en uno de los centros de rehabilitación social de varones determinado para el efecto, y se les descontará el tiempo que han permanecido detenidos por esta causa; además, se les impone a cada uno de ellos, conforme al principio de favorabilidad y el Art. 70.3 del COIP, la multa de 3 SBUTG, equivalente a la suma de USD $ 1.158 y que lo depositarán en la cuenta del BANCO DEL PACIFICO No. 7696256, sublínea 170499, a nombre de BCE-CCU-Dirección Provincial Consejo Judicatura Pichincha.- En cuanto a la reparación integral, de acuerdo con el Art. 78.3 Ibídem, como indemnización por daños materiales se dispone que los precitados ciudadanos paguen US$ 20.000,oo a la víctima NAGRAVISION S.A., de la siguiente manera BYRON PATRICIO BRIONES RIVAS US$ 15.000,oo y JORGE JAIRO GAVILANEZ ANCHUNDIA US$ 5.000,oo, dinero que debe ser pagado en forma inmediata; en cuanto a la reparación inmaterial los precitados ciudadanos deben publicar a través de la página web www.all.ec, a la cual estaban atados los links y foros en los cuales se ofertaba los servicios de IVS, que consiste en servicios en oferta de transmisión de televisión paga, y por un tiempo mínimo de un año una publicidad en donde se explique claramente que el servicio IKS y el servicio IPTV son retransmisiones ilegales, que para su acceso se ingresó ilegalmente y sin consentimiento de los generadores y propietarios de la señal de Televisión paga.- Actúe el Dr. Patricio Calderón, secretario de esta Unidad Judicial.- CUMPLASE Y NOTIFIQUESE.

Comentario del Autor

Del presente caso se puede destacar la evidente vulneración de la seguridad de los activos de los sistemas de información y comunicación y por ende el cometimiento de un delito informático, materia de análisis del presente trabajo de investigación, el mismo se desarrolla por el cometimiento del delito de acceso no autorizado a un sistema informático, telemático o de telecomunicaciones, mismo que se encuentra tipificado en el Código Orgánico Integral Penal, tras la denuncia, el allanamiento y detención de los ciudadanos implicados en el hecho. Se evidencia como los procesados a través de las TIC acceden a un sistema de telecomunicaciones privado y comienzan a ofertar los servicios que ofrece este sin ninguna autorización legitima del dueño, para ser específicos entraron a un dominio central de televisión

y ellos ofertaban planes de televisión más económicos, de esta manera se evidencia el cumplimiento de lo estipulado por el art 234 del COIP quien sanciona este delito, se evidencia que además ofertaban el servicio a nivel internacional. Finalmente, estas personas receptaban las ganancias de este delito mediante cuentas de diferentes entidades bancarias. Las partes procesales se sometieron a un procedimiento abreviado por la naturaleza del delito es factible hacerlo y por lo tanto en el mismo se sentencia con penas privativas de libertad y no privativas de libertad como lo son las multas.

En este caso podemos evidenciar la correcta aplicación de la ley penal en cuanto a delitos informáticos, pero esto es posible siempre y cuando los mismos delitos se encuentren tipificados y sancionados dentro del marco legal mediante leyes claras y concisas, como en este caso, la conducta cometida es sancionada por el Código Orgánico Integral Penal, si no fuera este el caso, estuviéramos evidenciando un caso más impune, es por esto que la sanción de estas conductas juegan un papel importante al momento de salvaguardar derechos y obligaciones de la ciudadanía.

6.3.2. Caso Nro. 2.

Datos Referenciales

Juicio No. 17282-2018-04178

Juzgado: Unidad Judicial de Garantías Penales de Pichincha

Procesado: Marco Vinicio Sandoval García

Actor: Fiscalía General del Estado

Delito: Art 232 Ataque a la Integridad de Sistemas Informáticos

Fecha: 29/04/2019

Antecedentes

La presente investigación se inicia con ayuda del Instituto Ecuatoriano de Seguridad Social mediante denuncia de la señora Maribel Cortez Estrella misma que indica que una de las usuarias del Instituto Ecuatoriano de Seguridad Social se acercó a ella para indicar que el señor Marco Vinicio Sandoval era la persona que realizaba actos informáticos en los cuales manipula el sistema informático de la institución, estos hechos permitían dar de baja las glosas o bajar las deudas que tenía las Instituciones. El señor procesado goza en calidad de funcionario de la Unidad de Coactivas. Un ejemplo de los hechos cometidos por el señor es con la empresa

Segurisarz, en donde se denota que dicha empresa tenía una deuda y al momento de bajar la glosa constaba sin deuda.

Con fecha 18 de diciembre de 2018, siendo las once horas con cincuenta minutos en la Sala de Audiencias de esta Unidad Judicial Penal de Pichincha con competencia en Infracciones Flagrantes, se llevó a cabo la Audiencia de Calificación de Flagrancia y Formulación de Cargos en contra de: SANDOVAL GARCÍA MARCO VINICIO. En donde Fiscalía, titular de la acción pública penal al tenor de lo establecido en el Art. 195 de la Constitución de la República del Ecuador y 410, 411 del Código Orgánico Integral Penal formuló cargos en contra del mencionado ciudadano por el delito de conforme al Art. 232 del Código Orgánico Integral Penal, esto es Ataque a la integridad de sistemas informáticos, dictándose en Audiencia a fin de garantizar la inmediación del procesado las medidas contempladas en el Art. 522 numerales 1 y 2. Con fecha 12 de abril del 2019 se celebró la Audiencia de Procedimiento Abreviado, en donde Fiscalía, solicitó el sometimiento al procedimiento abreviado dentro de la presente causa a favor del procesado que al momento de la referida audiencia, se puso en conocimiento por parte de Fiscalía que responde a los nombres de: SANDOVAL GARCÍA MARCO VINICIO, CON c.c. 1708073588, de nacionalidad ecuatoriana, de estado civil casado, de 54 años de edad, domiciliado en esta ciudad de Quito; acreditando todos los requisitos previstos, así como la determinación de la pena reducida acordada conforme a lo establecido en el Art. 635 y 636 del COIP. De igual manera refieren que las partes han convenido la pena privativa de la libertad de VEINTE MESES.

Resolución

ADMINISTRANDO JUSTICIA, EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR, Y POR AUTORIDAD DE LA CONSTITUCIÓN Y LAS LEYES DE LA REPÚBLICA, el suscrito Juez de la Unidad Judicial de Garantías Penales con sede en el Distrito Metropolitano de Quito, por existir probada la existencia de la infracción y la responsabilidad de los acusados, declara AUTOR responsable del delito previsto en el Art. 232 del COIP, esto es de ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS, de conformidad con el Art. 42 numeral 1 literal a) al señor: SANDOVAL GARCÍA MARCO VINICIO, CON c.c. 1708073588, de nacionalidad ecuatoriana, de estado civil casado, de 54 años de edad, domiciliado en esta ciudad de Quito, VEINTE MESES de pena privativa de libertad. La Pena que cumplirán conforme a lo establecido en el COIP en lo que refiere a la ejecución de penas. En lo referente al Artículo 70 del COIP se aplica la multa al sentenciado CIFUENTES PRADA

JONATHAN, con documento de identificación No. CEDF124463, de nacionalidad colombiana, de 27 años de edad, de estado civil unión de hecho, de doce salarios básicos; es menester indicar que al encontrarnos los ecuatorianos bajo el marco de "un Estado Constitucional de derechos y justicia", el juzgador, necesariamente debe acatar el principio de legalidad, esto es que debemos aplicar lo que invoca la ley, en el caso en particular, el artículo 70 del COIP, refiere: "En las infracciones previstas en este Código se aplicará además la pena de multa conforme con las siguientes disposiciones". En el caso sub judice, la pena prevista es la determinada en el artículo 232 del COIP, que va de 3 a 5 años, la multa a aplicarse por tanto es la invocada en el numeral 5 en razón del principio de proporcionalidad de la pena privativa de libertad frente a la pena accesoria como es la multa, por lo cual se impone ocho salarios básicos del trabajador en general, debiendo depositar dicho valor en la cuenta No. 7696256, sub línea No. 130130, del Banco del Pacífico perteneciente al "BCE CCU DIRECCIÓN PROVINCIAL DEL CONSEJO DE LA JUDICATURA PICHINCHA. DE LA REPARACION INTEGRAL. - El artículo 78 de la Constitución de la República reconoce el derecho a la reparación integral, al efecto señala: "Las víctimas de infracciones penales gozarán de protección especial, se les garantizará su no revictimización, particularmente en la obtención y valoración de las pruebas, y se las protegerá de cualquier amenaza u otras formas de intimidación. Se adoptarán mecanismos para una reparación integral que incluirá, sin dilaciones, el conocimiento de la verdad de los hechos y la restitución, indemnización, rehabilitación, garantía de no repetición y satisfacción del derecho violado…"; norma que se encuentra en concordancia, con el numeral 6 del artículo 622 del Código Orgánico de la Función Judicial que establece como requisito de la sentencia: "La condena a reparar integralmente los daños ocasionados por la infracción con determinación del monto económico que pagará la persona sentenciada a la víctima y demás mecanismos necesarios para la reparación integral, con determinación de las pruebas que hayan servido para la cuantificación de los perjuicios cuando corresponda"; y, el primero inciso del artículo 628 del COIP, el mismo que determina que "Toda sentencia condenatoria deberá contemplar la reparación integral de la víctima, con la determinación de las medidas por aplicarse, los tiempos de ejecución y las personas o entidades públicas o privadas obligadas a ejecutarlas…".- Dentro de la presente causa al tratarse de tipo penal juzgado, como mecanismo de reparación se encuentra el conocer la verdad de los hechos de conformidad con lo realizado por el fiscalía en su investigación, lo que conllevó a la presente sentencia en contra del infractor; de igual forma, es preciso indicar que al ser la vulneración de un sistema informático de una institución estatal, el IESS debe adoptar las medidas de seguridad informática y protocolos pertinentes que impidan, y alerten a los

departamentos pertinentes de dicha institución, la vulneración, alteración y cualquier tipo de irregularidad análoga al caso que se resuelve en este sentencia. Conforme lo determina el Art. 64 numeral 2 de la Constitución de la República, en concordancia con el Art. 60 numeral 13 del Código Orgánico Integral Penal, se suspenden los derechos de participación de la sentenciada por un tiempo igual al de la condena, comuníquese del particular a las autoridades pertinentes. Actúe como Secretario de esta Unidad Judicial la Dra. María José Rivadeneira Domínguez.

Comentario del autor:

En este caso evidenciamos otro tipo de delito informático, incluso algo diferente dentro de la categoría dogmática puesto que quien lo cometió era servidor de la entidad afectada, configurando esto un sujeto activo especial. En este caso se comete el delito tipificado en el artículo 232 del Código Orgánico Integral Penal, este delito describe varias conductas, ahora parte concreta de este delito la encontramos donde se especifica la supresión total o parcial de contenido digital, que en este caso el procesado eliminaba las deudas de empresas con la institución afectada, recayendo en el artículo antes mencionado, vemos la correcta aplicación de las leyes penales y la sanción impuesta por el juzgador se la aplica de acuerdo a todo en lo que derecho fue actuado. De esta manera se evidencia la eficiencia del sistema legal en cuanto existen delitos tipificados en el sistema penal. Estos delitos por su fácil cometimiento aumentan, sin embargo, por el oportuno actuar de la justicia como en este caso se puede contrarrestar estas conductas dañinas, que aparte de afectar la integridad de la información y los sistemas informáticos, también dañan y vulneran el patrimonio.

6.3.3. Caso Nro. 3.

Título: Agencia de viajes colombiana alerta sobre estafas en Ecuador a través de redes sociales.

Fecha: 09 de julio de 2024

Lugar: Ecuador

Link de la noticia: https://www.primicias.ec/noticias/sucesos/estafa-agencia-viajes-redes-sociales-suplantacion-colombia/

Contenido:

Una familia de Ecuador adquirió un paquete vacacional a Punta Cana, en República Dominicana, tras contactar a una supuesta agencia de viajes por redes sociales.

Daniela, mujer afectada, contó -al canal de televisión Teleamazonas- que la agencia que encontró se llamaba Wakanda Travel. Tras cerrar el negocio, recibió un supuesto contrato y pagó el 50% del costo del paquete.

Pero luego le pidieron pagar USD 400 más, porque supuestamente había subido el costo de los pasajes. Este hecho alertó a Daniela de que algo no estaba bien (Beltrán, 2024, p. 1).

Al momento de ir a denunciar en Fiscalía, se enteraron que no había sido el único caso de esta estafa, la denuncia fue planteada el 08 de julio del presente año.

Comentario del Autor:

La situación descrita en el caso de la familia ecuatoriana estafada por una supuesta agencia de viajes en redes sociales refleja un problema creciente de estafas informáticas y engaños en plataformas digitales. Este tipo de estafa pone de manifiesto la necesidad de una mayor regulación y supervisión de las actividades comerciales en internet, así como la importancia de la educación y concienciación de los consumidores sobre los riesgos asociados con las transacciones en línea.

Desde una perspectiva jurídica, el caso de Wakanda Travel no podría tipificarse como un delito de estafa, contemplado en el artículo 186 del Código Orgánico Integral Penal (COIP) de Ecuador. Este artículo sanciona a quienes, mediante engaño, obtienen un beneficio económico en perjuicio de otra persona. La modalidad de la estafa en este caso involucra el uso de medios electrónicos, lo que añade una capa de complejidad y resalta la necesidad de capacidades especializadas en la investigación y persecución de delitos informáticos y este delito no se encuentra tipificado en el país.

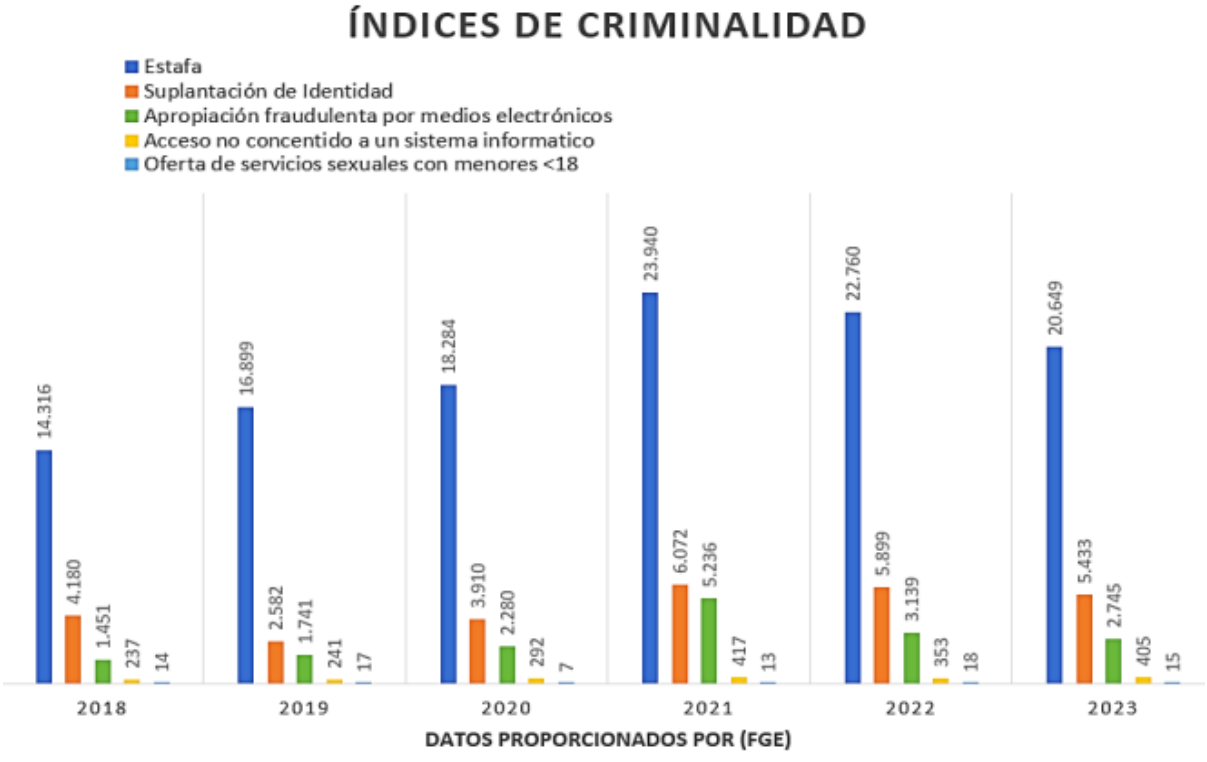
La denuncia presentada por Daniela y otras víctimas ante la Fiscalía es un paso crucial para iniciar el proceso de investigación y eventual sanción de los responsables. Es fundamental que las autoridades competentes utilicen herramientas de investigación cibernética para rastrear y desmantelar las operaciones fraudulentas, protegiendo así a los ciudadanos de futuras estafas.

Este caso es un ejemplo ilustrativo de cómo las estafas en línea pueden afectar a los ciudadanos y la necesidad de leyes más robustas y específicas para combatir estos delitos.

En resumen, la estafa perpetrada por la página falsa de Wakanda Travel es un llamado de atención sobre la vulnerabilidad de los consumidores en el entorno digital y la urgente necesidad de fortalecer el marco jurídico para combatir eficazmente los delitos informáticos, protegiendo así los derechos e intereses de los ciudadanos.

6.4. Análisis de datos estadísticos

Para el desarrollo del análisis estadístico se ha procedido a obtener información emitida por la Fiscalía General del Estado.



Fuente: Fiscalía General del Estado

Comentario del Autor:

Las estadísticas presentadas sobre los índices de criminalidad relacionados con delitos informáticos en Ecuador, basadas en datos proporcionados por la Fiscalía General del Estado, muestran una tendencia preocupante en varios tipos de crímenes cibernéticos desde 2018 hasta 2023. La estafa ha mostrado un incremento significativo desde 2018, alcanzando su punto más alto en 2021 con 23,940 casos, y manteniéndose elevada en los años siguientes con 22,760 casos en 2022 y 20,649 en 2023, lo que sugiere una necesidad urgente de fortalecer las medidas preventivas y las sanciones para disuadir este tipo de delitos. La suplantación de identidad ha tenido un crecimiento más moderado pero constante, pasando de 1,451 casos en 2018 a 5,433 en 2023, reflejando la creciente sofisticación y prevalencia de técnicas utilizadas para cometer estos delitos, indicando la necesidad de mejorar la educación pública sobre la protección de datos personales. Aunque los casos de apropiación fraudulenta por medios electrónicos son menos numerosos, han mostrado un aumento en los últimos años, con 2023 registrando 3,745 casos, destacando la necesidad de una mayor vigilancia y regulación de las transacciones

electrónicas. El acceso no consentido a un sistema informático ha tenido cifras relativamente bajas en comparación con otros, pero sigue siendo relevante con 405 casos en 2023, subrayando la importancia de la ciberseguridad y la protección de sistemas informáticos contra accesos no autorizados. Los casos de oferta de servicios sexuales con menores de 18 años se mantienen bajos pero persistentes, con fluctuaciones anuales y alcanzando 105 casos en 2023, requiriendo una atención particular debido a su gravedad y el impacto en las víctimas. En conclusión, las estadísticas de delitos informáticos en Ecuador resaltan una tendencia al alza en varios tipos de crímenes cibernéticos, en especial la estafa, esto nos indica la necesidad de respuestas más robustas y coordinadas para proteger a los ciudadanos y las instituciones del país como una reforma al Código Orgánico Integral Penal en donde se incluya este delito para así contrarrestar esta actividad ilícita.

7. Discusión

7.1. Verificación de objetivos

Para la elaboración del presente Trabajo de Integración Curricular se estableció un objetivo general, tres objetivos específicos, que se detallan a continuación.

7.1.1. Verificación del objetivo general

El objetivo general propuesto es **"Realizar un estudio jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal".**

El objetivo general de este estudio ha sido debidamente verificado a lo largo del desarrollo del marco teórico, puesto que, se llevó a cabo un análisis exhaustivo y puntualizado del tema, apoyándose en fuentes que van desde los diccionarios jurídicos, doctrina, legislación vigente, acuerdos o reglamentos internacionales y legislación vigente de Colombia, Perú y Costa Rica. Mediante el uso de los diccionarios jurídicos, la doctrina y la legislación internacional, se abordaron y desarrollaron todos los aspectos concernientes a este objetivo y se ha comprobado que realmente existen conductas dañosas tipificadas en las legislaciones vecinas, que ocurren en el país, sin embargo, no han sido tomadas en cuenta por el legislador nacional para ser agregadas al Código Orgánico Integral Penal.

Los temas que es pertinente a destacar son, la Terminología jurídica, especialmente el término Derecho Informático, Delito, Delito Informático, Estafa Informática y Facilitación del delito informático.

Además, se destacó la necesidad de un marco regulatorio para proteger los derechos fundamentales en el contexto de las crecientes olas de delitos informáticos no tipificados dentro del Ecuador.

En este ámbito se ha podido comprender todo lo concerniente a los delitos informáticos o ciberdelitos, considerando no solamente la legislación nacional, sino que también se puntualizó lo que las legislaciones extranjeras nos refieren al respecto, pudiendo comprender de esta manera que este campo de la informática como lo son los delitos informáticos se deben analizar con mucha cautela, y es necesario que el Estado como ente regulador de derechos, establezca limitaciones en nuestro país, porque es algo que está avanzando a pasos agigantados y se debe tener la pena certeza que la ciudadanía cuenta con seguridad jurídica y no se vea en la terrible situación de no poder acudir ante la ley porque no hay una norma que sancione estos delitos.

El análisis que se pudo evidenciar, ha permitido conocer todo lo relacionado al Delito, Delito Informático, Derecho informático, y elementos del mismo, además de entender a fondo las acciones ilícitas no tipificadas en el Ecuador. Todos los temas y subtemas que se encuentran en el marco teórico, se ajustan a la problemática plantada, brindando con ello, un estudio absoluto de lo que conlleva estos ilícitos que es dañar gravemente derechos como la propiedad, patrimonio, intimidad, seguridad de los sistemas de información. Fundamentación jurídica de la propuesta de reforma legal.

En lo que se refiere al estudio jurídico se lo realizó a través de un análisis e interpretación determinante de las normas jurídicas que se encuentran relacionadas con los delitos informáticos, se puede partir de la constitución en donde se encuentran los derechos que son vulnerados al ser víctimas de estas acciones. Por esto es que se tuvo en cuenta en la Constitución de la República del Ecuador, el Código Orgánico Integral Penal, la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos y la Ley de Comercio Electrónico, Firmas y Mensajes de Datos; como normativa nacional y pertinente, y, como normativa legal extranjera se tomó en cuenta a Colombia, Perú y Costa Rica, con el Código Penal de Colombia, Ley de Delitos Informáticos Ley 30096 del Perú y el Código Penal de Costa Rica respectivamente.

Al examinar la legislación nacional e internacional, se busca identificar las mejores prácticas y los principios fundamentales que deben guiar la regulación de los delitos informáticos, en este caso la estafa informática y la facilitación del delito informático. Se evalúan algunos aspectos clave como el respeto a la propiedad, el patrimonio, la seguridad, la legalidad de estas acciones,

la seguridad de los sistemas de información y comunicación, la garantía de protección de los derechos individuales y la prevención del abuso de la tecnología.

7.1.2. Objetivos específicos

1. **"Demostrar que la falta de tipificación y sanción en la legislación penal ecuatoriana de algunas conductas dañosas cometidas mediante medios informáticos permiten la impunidad."**

Este objetivo específico se pudo verificar acorde a lo establecido en la primera y cuarta pregunta de la encuesta, puesto que la mayoría de los encuestados, respondieron que sí, que estas conductas dañosas al estar tipificadas evitarían la impunidad de las mismas, por ende, al no encontrase tipificadas ni sancionadas, estos hechos ilícitos, se permite la impunidad de los mismos, permitiendo a los ciberdelincuentes hacer daño a la gente y a los sistemas informáticos, además los administradores de justicia no tienen en donde fundamentarse para poder realizar su trabajo. Un punto a destacar es que los encuestados afirman que la tipificación de manera independiente de estos delitos permite una descripción más precisa de las conductas delictivas, lo cual facilita su identificación y enjuiciamiento, esto reduce la ambigüedad legal y mejora la capacidad de las autoridades para perseguir estos crímenes, ahora bien, en las respuestas de la cuarta pregunta se refleja que si se sanciona y tipifica estas acciones si se disminuiría el índice de estos hechos delictivos; Por su parte, este objetivo de igual forma se verifica con la primera y cuarta pregunta de la entrevista, en donde los entrevistados determinaron que la no existencia de estas conductas permite la impunidad de estas acciones, además se destaca la necesidad urgente de ampliar las herramientas legales para poder combatir contra estas actividades ilícitas y al agregar estas conductas a la norma penal se reducirá notablemente la delincuencia informática; A su vez, este objetivo, se verifica con el derecho comparado entre Colombia, Perú y Costa Rica, puesto que en el contexto costarricense se fomenta un marco legal más detallado acerca de los delitos informáticos, tipificando y sancionando conductas como la estafa informática y la facilitación del delito informático, protegiendo de esta forma bienes jurídicos primordiales. La comparación entre estas legislaciones permitió identificar los pros y contras del sistema penal ecuatoriano, con relación a la ley penal de otros países. Finalmente, en el estudio de casos concluimos que, los delitos pueden ser contrarrestados siempre y cuando se encuentren debidamente tipificados por la ley, ya que de esta manera se puede sancionar estas conductas y de esta manera se protege y se repara a la victima de estos hechos, caso contrario ocurre con la estafa informática, estos ilícitos ocurren a diario y crecen de manera desacelerada,

afectando así derechos protegidos en la constitución y demostrando que la falta de la tipificación de esta conducta permite que los ciberdelincuentes queden impunes y a las víctimas no se les repara de ninguna forma el daño ocasionado.

2. "Determinar algunas conductas que deben ser tipificadas y sancionadas en el Código Orgánico Integral Penal para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana."

Siguiendo con el este objetivo, se puede verificar mediante la aplicación de encuestas y entrevistas, exactamente con la segunda pregunta de las mismas, en donde los encuestados y entrevistados nos refieren que para poder garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana si es necesario tipificar y sancionar conductas que si se encuentran en la legislación extranjera, , ya que de esta manera se proporcionaría claridad y precisión en la ley permitiendo un procesamiento más efectivo de estos delitos y se protegería adecuadamente los derechos de las víctimas, en específico las personas encuestadas y entrevistadas en su gran mayoría optaron por agregar al COIP los delitos de estafa informática y facilitación del delito informático, los cuales según ellos, no son perseguidos por falta de normativa legal, impidiendo el ejercicio de derechos de los ecuatorianos.

3. "Presentar una propuesta de reforma legal incorporando nuevos delitos informáticos."

El último objetivo específico se logró verificar con los resultados obtenidos con las cuatro primeras preguntas de las entrevistas y encuestas, en las cuales, se resalta el gran acuerdo que existe en reformar el Código Orgánico Integral Penal tipificando y sancionando delitos informáticos, los resultados indican que los delitos que deberían ser tomados en cuenta por la Asamblea Nacional, serian la estafa informática y la facilitación del delito informático, los entrevistados hacen énfasis en que las TIC han ayudado y aportado mucho para el desarrollo de la sociedad, sin embargo también son usadas para el cometimiento de delitos y que como la tecnología avanza, también debería avanzar el derecho adaptándose a las nuevas realidades que surgen dentro de la sociedad.

El derecho comparado nos muestra y nos ayuda en cómo se debería implementar la reforma legal del COIP, pues de la legislación de Costa Rica es de donde se obtiene los delitos que en Ecuador no se encuentran tipificados, esto resulta muy significativo para poder establecer un marco legal claro y preciso dentro de la legislación ecuatoriana.

8. Conclusiones

Una vez realizado el marco teórico y luego de haber analizado los resultados de las técnicas de acopio empírico, como lo son las encuestas y las entrevistas, y otros elementos indispensables para el desarrollo de este trabajo de integración curricular, he llegado a las siguientes conclusiones:

Primera: Se ha logrado evidenciar el gran desarrollo dentro del estado ecuatoriano en cuanto a la sanción y tipificación de ciberdelitos, sin embargo, aún existen algunas carencias que permiten la impunidad de algunas acciones que en la legislación extranjera como en es la de Costa Rica si son tomadas en cuenta. Por su parte, Perú y Colombia en sus cuerpos normativos respectivos penalizan las mismas acciones delictivas que son tomadas en cuenta por el legislador ecuatoriano, solo se diferencian en algunos verbos rectores y en las penas, sin embargo, tienen el mismo fin.

Segunda: Según los resultados de las encuestas y las entrevistas se logra destacar que la falta de tipificación y sanción de algunas conductas que en el extranjero son tomadas en cuenta como delitos informáticos, permite la impunidad de las mismas y de esta manera no se garantiza el ejercicio pleno de los derechos de la ciudadanía ecuatoriana.

Tercera: La tendencia en cuanto a delitos informáticos se mantiene en un nivel preocupante, sin embargo, esto es contrarrestado por las leyes vigentes del país, por otro lado, la tendencia en cuanto a estafas por medios informáticos va al alza, esto como resultado de la no tipificación de esta conducta como un delito independiente dentro del Código Orgánico Integral Penal.

Cuarta: Se ha logrado verificar los objetivos propuestos de manera correcta, puesto que en el desarrollo de la presente investigación se logró demostrar la falta de tipificación y sanción de delitos informáticos, mismos que se determinaron como la estafa informática y la facilitación del delito informático.

Quinta: Mediante el estudio de casos se logró determinar que en el Ecuador se logra contrarrestar y juzgar correctamente los delitos informáticos, siempre y cuando los jueces tengan bases jurídicas para juzgar, como lo es correcta tipificación de los acciones que son tomados como delitos informáticos, caso contrario es cuando no existe la sanción de alguna conducta permitiendo que los ciberdelincuentes operen sin restricción, violando derechos de la ciudadanía, evitando así la correcta administración de justicia por parte del estado ecuatoriano.

Sexta: En el Ecuador al no existir regulación jurídica con respecto a la estafa informática y la facilitación de delito informático se es necesaria una reforma al Código Orgánico Integral Penal incluyendo estas conductas para su correcto juzgamiento y sanción, fortificando de esta manera el sistema judicial y la seguridad jurídica frente a este creciente problema.

9. Recomendaciones

En base a las conclusiones, se llega a las siguientes recomendaciones para abordar la problemática establecida:

Primera: Al Estado Ecuatoriano, se recomienda estar a la par de legislaciones vecinas en cuanto a la tipificación de delitos informáticos, como el de Costa Rica, puesto que esta materia se encuentra en constante desarrollo, logrando de esta manera un marco legal claro y actualizado para que con esto se logre mitigar el mal uso de las tecnologías de la información y la comunicación.

Segunda: A la Fiscalía General del Estado, implementar mecanismos de denuncia y reporte efectivos, programas de educación y conciencia sobre la seguridad en la sociedad de la información, además se recomienda la capacitación del personal de fiscalía en cuanto a delitos informáticos para así garantizar una mejor investigación y persecución de estos hechos garantizando a la ciudadanía seguridad jurídica con respecto a su entorno digital**.**

Tercera: Al Ministerio de Educación, desarrollar programas educativos acerca de las practicas dañinas que se realizan a través de sistemas informáticos par así generar conciencia sobre las actividades ilícitas por medios informáticos, de igual manera capacitar a docentes y demás personal administrativo acerca de las modalidades de los delitos informáticos para así evitar que estos sean víctimas de los ciberdelincuentes.

Cuarta: A las instituciones de educación superior como las universidades públicas y privadas, fomentar actividades e investigaciones acerca de la seguridad y riesgos informáticos, además capacitarlos acerca de las consecuencias jurídicas que traen consigo estas conductas delictivas. Se recomienda también mantenerse actualizados acerca del desarrollo de nuevos delitos informáticos y como prevenirlos, garantizando así seguridad para los estudiantes y para el personal de las universidades.

Quinta: Al Estado Ecuatoriano, destinar fondos en la inversión de medios tecnológicos de última generación, capacitaciones para la policía y fiscalía en las unidades correspondientes a

la persecución de delitos informáticos para contribuir a la correcta persecución y evitar dejar impunes estas conductas.

Sexta: A la Asamblea Nacional, que acepte el siguiente proyecto de ley propuesto para reformar el Código Orgánico Integral Penal, tipificando los delitos como la estafa informática y la facilitación del delito informático, reforzando el sistema jurídico en la lucha contra los delitos informáticos y garantizando la seguridad jurídica para que los jueces puedan sustentar y fundamentarse en lo legal al momento de juzgar estos delitos.

9.1.Propuesta de Reforma Legal

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

LA ASAMBLEA NACIONAL DEL ECUADOR

CONSIDERANDO:

Que, el artículo 1 de la Constitución de la República del Ecuador declara que el Ecuador es un Estado constitucional de derechos y justicia siendo fundamental el respeto a esta garantía;

Que, el artículo 16 de la Constitución de la República del Ecuador reconoce el derecho de todos los ciudadanos al acceso universal a las tecnologías de información y comunicación, así como a la creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de frecuencias del espectro radioeléctrico y a bandas libres para la explotación de redes inalámbricas;

Que, nuestra Carta Magna en su artículo 17 numeral 2 dispone que el Estado se encargará de fomentar la pluralidad y diversidad en la comunicación, y, además, facilitará el acceso universal a las tecnologías de la información y comunicación en especial para las personas y colectividades que arezcan d dicho acceso o lo tengan de forma limitada;

Que, el artículo 66 numeral 19 de la Constitución de la República del Ecuador reconoce y garantiza a las personas 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;

Que, el artículo 82 de la Constitución de la República del Ecuador reconoce que el derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

Que, el artículo 22 de la Ley de Comunicación establece que todas las personas tienen derecho a que la información de relevancia pública que reciben a través de los medios de comunicación sea verificada, contrastada, precisa y contextualizada.

Que, el artículo 186 del Código Orgánico Integral Penal establece que la persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

Que, en el ejercicio de sus atribuciones, la Asamblea Nacional, de acuerdo al Art. 84 de la Constitución de la República del Ecuador, tiene la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y respectivamente en los tratados internacionales.

Que, el inciso 1, del Art. 5, del Código Orgánico Integral Penal sobre el principio de legalidad manifiesta: “No hay infracción penal, pena, ni proceso penal sin ley anterior al hecho”.

Que, el Código Orgánico Integral Penal, en el Art 13 establece normas de interpretación: 1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando al sentido literal de la norma. 3. Queda prohibida la 75 utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide lo siguiente:

LEY REFORMATORIA AL CÓDIGO ORGÁNICO INTEGRAL PENAL

Artículo uno. – A continuación del articulo 234.4 agréguese dos innumerados con el siguiente texto:

Artículo (234.5). - Estafa Informática.

Serán sancionados con pena privativa de libertad de tres a cinco años quien, en perjuicio de una persona natural o jurídica:

1. Manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro, induciendo al error a otra persona para que realice un acto que perjudique su patrimonio o el de una tercera.
2. Cree cuentas falsas en redes sociales o plataformas digitales con el propósito de vender productos o servicios inexistentes, logrando así engañar y apropiarse de bienes o dinero de las personas que realizan transacciones creyendo en la veracidad de dichas ofertas.

Se impondrá pena privativa de libertad de cinco a siete años si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo (234.6). - Facilitación del delito informático. Se impondrá pena privativa de libertad de uno a tres años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

DISPOSICIÓN FINAL.

ÚNICA. - La presente reforma entrará en vigor a partir de la fecha de su publicación en el Registro Oficial.

Dado en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los cinco días del mes de agosto del año dos mil veinticuatro.

MSC. HENRY FABIAN KRONFLE KOZHAYA
Presidente de la Asamblea Nacional

ABG. ALEJANDRO MUÑOZ HIDALGO
Secretario General

10. Bibliografía

Acuario, S. (2016). *Delitos Informáticos: Generalidades.*

Aguilar, P. A. (2015). ¿Derecho Informático ó Informática Jurídica? *Revista de investigación en tecnologías de la información, III*, 19-24.

Albán, E. (2018). *Manual de Derecho Penal Ecuatoriano* (Tercera ed.). Quito, Pichincha, Ecuador: Ediciones Legales EDLE S.A. https://doi.org/978-9978-81-190-0

Alcívar Trejo, C., Domenech Alvarez, G., y Ortiz Chimbo , K. (2015). La Seguridad Jurídica frente a los Delitos Informáticos. *AVANCES, Revista de Investigación Jurídica*, 1-17.

Asamblea legislativa de la república de Costa Rica. (1970). *Código Penal.*

Asamblea Nacional del Ecuador. (31 de Marzo de 2010). Asamblea Nacional del Ecuador.

Beltrán, J. (09 de Julio de 2024). Agencia de viajes colombiana alerta sobre estafas en Ecuador a través de redes sociales. *Primicias*. https://www.primicias.ec/noticias/sucesos/estafa-agencia-viajes-redes-sociales-suplantacion-colombia/

Cabanellas, G. (2005). *Diccionario Jurídico Elemental.* Heliasta.

Casado, L. (2008). *Diccionario de Derecho.* Valleta Ediciones. https://doi.org/978-950-743-308-5

Castillo, J. (2022). Incidencia en la Criminalidad por la Limitación del Uso de Armas de Fuego Dotadas por el Estado a la Policía Nacional y por la Falta de Medios y Armas Adecuadas a los Agentes de Seguridad Penitenciaria. *[Trabajo de Integración Curricular previo a la obtención del título de abogada].* Universidad Nacional de Loja, Loja, Loja, Ecuador. https://doi.org/https://dspace.unl.edu.ec/jspui/handle/123456789/25311

Céspedes, J. F. (2000). El Derecho Informático frente a la contratación electrónica. En J. F. Céspedes, *Revolución Informática con Independencia del Individuo* (pp. 292-300). RAO.

Código Orgánico Integral Penal. (2014).

Congreso de Colombia. (2000). *Código Penal de Colombia.*

Congreso de Colombia. (2009). *Ley 1273 de 2009.*

Congreso de la República del Perú. (2013). *Ley de Delitos Informáticos Ley 30096.* Retrieved 23 de Julio de 2024.

Constitución de la República del Ecuador. (2008). Registro Oficial.

Constitución Política del Perú. (1993).

Couture, E. J. (2006). *Diccionarios Vocablo Jurídico.*

Diario Crónica. (02 de Marzo de 2023). ¿Cómo prevenir los delitos informáticos? *Crónica las noticias al día*. https://cronica.com.ec/2023/03/02/como-prevenir-los-delitos-informaticos/

El Comercio. (25 de Julio de 2022). 3183 delitos informáticos se han registrado en el Ecuador, desde el 2020. *3183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. El Comercio: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

El Congreso de Colombia. (2009). *Ley 1341 de 2009.*

El Universo. (27 de Septiembre de 2020). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. *El Universo*, p. 1. https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador/#:~:text=Los%20m%C3%A1s%20frecuentes%20son%20las,pedir%20dinero%20a%20sus%20contactos.

El Universo. (4 de Agosto de 2021). Conozca cuáles son los delitos informáticos con pena de prisión en Ecuador. *El Universo*.

Espinoza, M. (2018). El Derecho Penal Informático Humano como cautela frente al Poder Punitivo en la Sociedad de Control. *Revista Derecho, III*, 233-245. https://doi.org/233-245

Fernández, H. (2016). *Manual de Derecho Informático.* Buenos Aires: AbeledoPerrot.

Fiscalía General del Estado. (03 de Marzo de 2023). *Fiscalía General del Estado*. Fiscalía obtiene sentencia por los delitos de acceso no consentido a un sistema informático,

telemático o de telecomunicaciones y revelación ilegal de base de datos: https://www.fiscalia.gob.ec/fiscalia-obtiene-sentencia-por-los-delitos-de-acceso-no-consentido-a-un-sistema-informatico-telematico-o-de-telecomunicaciones-y-revelacion-ilegal-de-base-de-datos/

Fiscalia General del Estado. (s.f.). *Fiscalia General del Estado*.

García, V. C. (12 de Mayo de 2023). *DPL news*. DPL news: https://dplnews.com/las-tic-ya-son-derecho-fundamental-en-costa-rica-a-un-ano-de-gobierno-rodrigo-chaves/#:~:text=A%20un%20a%C3%B1o%20de%20haber,TIC)%20como%20un%20derecho%20fundamental.

Girón, J. G. (2021). *Teoría del Delito.*

Imbaquingo Narváez, H. S., Imbaquingo Esparza, D. E., Arciniega Hidrobo, S. R., Jácome León, J. G., Ron Egas, M. B., Ortega Bustamante, C. M., y Ayala Bermeo, J. A. (2019). *Derecho Informático y Nuevas Tecnologías de la Información.* Ibarra, Imbabura, Ecuador: Imprenta Universitaria . Retrieved 05 de Julio de 2024.

Legal Center Abogados. (2022). Legal Center Abogados : https://legalcentercr.com/derecho-informatico/#:~:text=El%20derecho%20inform%C3%A1tico%20en%20Costa,actividades%20realizadas%20en%20el%20ciberespacio.

Ley de Comercio Electrónico, Firmas y Mensaje de Datos. (2002).

Machado, J. (10 de Junio de 2024). EL 8,2% de ecuatorianos son analfabetos digitales y eso los hace vulnerables", según policía de ciberdelitos. *Primicias*, p. 1. https://www.primicias.ec/noticias/seguridad/ciberdelitos-ecuador-estafas-analfabetos-digitales-vulnerables/#:~:text=Estos%20delitos%20ocurren%20cuando%20las,2022%3B%20y%2067%20en%202023.

MedlinePlus. (23 de Mayo de 2024). *MedlinePlus* . Información para su salud: https://medlineplus.gov/spanish/sleepdisorders.html#:~:text=El%20sue%C3%B1o%20es%20un%20complejo,saludable%20y%20se%20sienta%20bien.

Montero, J. E. (2023). La Teoría del Delito. *Lecciones de Derecho Penal Ecuatoriano, I*, 59-72.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2022). *Compendio de Ciberdelincuencia Organizada.* Viena: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

OMS. (8 de Junio de 2022). *Organización Mundial de la Salud*. Trastornos Mentales: https://www.who.int/es/news-room/fact-sheets/detail/mental-disorders

ONU, A. G. (1948). *Declaración Universal de los Derechos Humanos.*

ONU, A. G. (2018). *Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluidos el derecho al desarrollo. .*

Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Hallazgos21, IIII*(1), 100-112.

Ossorio, M. (2008). *Diccionario de Ciencias Jurídicas Políticas y Sociales.* Heliasta.

Real Academia Española. (2023). *Diccionario de la lengua española.* [versión 23.7 en línea]. https://doi.org/https://dle.rae.es/ciberdelincuencia?m=form

Real Academia Española. (2023). *Diccionario de la lengua española.* https://dle.rae.es/seguridad?m=form#EMJI0mh

Real Academia Española. (19 de Julio de 2024). *Real Academia Española*. Diccionario de la lengua española: https://dle.rae.es/ciberdelito

Salazar, L. (12 de Noviembre de 2013). *Tecnología y Derecho*. Tecnología y Derecho: https://tecnologiaenelderecho.weebly.com/blog/importancia-del-derecho-informtico

Téllez, J. (2008). *Derecho Informático.* México, D. F.: McGRAW-HILL/INTERAMERICANA EDITORES, A.A. DE C.V. https://doi.org/ISBN-13: 978-970-10-6964-6

Tixi, S. (2022). Análisis dogmático jurídico respecto a los delitos informáticos en el Código Orgánico Integral Penal. *[Tesis de maestría].* Universidad Regional Autónoma de los Andes, Ambato. https://doi.org/https://dspace.uniandes.edu.ec/handle/123456789/14631

UNDOC. (2024). *Oficina de las Naciones Unidas contra la Droga y el Delito*. UNDOC: https://www.unodc.org/e4j/es/tertiary/cybercrime.html

11. Anexos

Anexo 1. Cuestionario de la Encuesta

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENCUESTA DIRIGIDA A PROFESIONALES DEL DERECHO, CONOCEDORES DEL PROBLEMA Y ESPECIALISTAS EN INFORMÁTICA

Distinguido/a: Me encuentro realizando mi Trabajo de Integración Curricular previo a la obtención del Título de Abogado. El tema que estoy desarrollando es el siguiente: "Análisis jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal." Para avanzar en esta investigación, solicito su valioso aporte a través de la presente encuesta. La información recabada es únicamente con fines académicos y será tratada con la debida confidencialidad. De antemano le agradezco por participar en esta encuesta.

Problema de investigación: En la era actual, los delitos informáticos están tomando fuerza debido a que las Tecnologías de la Información y la Comunicación se desarrollan de manera muy acelerada y de igual forma se van acoplando a este desarrollo los ciberdelincuentes que explotan estas nuevas tecnologías con el fin de realizar actos nocivos y dañinos para la ciudadanía y como es de conocimiento general, actualmente toda persona ya sea natural o jurídica, tiene como mínimo un dispositivo tecnológico en su hogar o en su lugar de trabajo, lo que los hace vulnerables a ser víctimas de estas acciones. Estos actos o conductas afectan ciertos bienes jurídicos como el patrimonio, la privacidad, la intimidad, etc. En Ecuador la tipificación de delitos informáticos ha sido algo ineficiente, por ende, es necesario realizar una comparación entre legislaciones para poder analizar y encontrar tipos penales que no están en nuestra legislación y así poder plantear una nueva reforma al Código Orgánico Integral Penal para sancionar nuevos ciberdelitos y de esta manera garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana.

ENCUESTA

1. **En otras legislaciones a diferencia de Ecuador se tipifica y sanciona así: en la Legislación Penal de Costa Rica la estafa informática y facilitación de delito**

informático. ¿Estima usted que la tipificación y sanción como delitos independientes de estas conductas en el Código Orgánico Integral Penal evitarían la impunidad?

SI ☐ **NO** ☐

¿Por qué?

……

……

……

……

……

2. **Considera usted que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delitos independientes:**

a) **Estafa Informática**

b) **Facilitación de delito informático**

¿Por qué?

……

……

……

……

……

3. **¿Está usted de acuerdo en Reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación penal extranjera constituyen delitos informáticos?**

SI ☐ **NO** ☐

¿Por qué?

……

……

……

……

……

4. **¿Considera usted que tipificando y sancionando las conductas descritas anteriormente se disminuiría el índice de la delincuencia que delinque utilizando medios informáticos?**

SI ☐ **NO** ☐

¿Por qué?

……

……

……

……

……

5. **¿Qué sugiere frente al problema planteado?**

……

……

……

……

……

Anexo 2. Cuestionario de Entrevista

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA DIRIGIDA A PROFESIONALES DEL DERECHO, CONOCEDORES DEL PROBLEMA Y ESPECIALISTAS EN INFORMÁTICA

Distinguido/a: Me encuentro realizando mi Trabajo de Integración Curricular previo a la obtención del Título de Abogado. El tema que estoy desarrollando es el siguiente: "Análisis jurídico y doctrinario de los delitos informáticos tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal." Para avanzar en esta investigación, solicito su valioso aporte a través de la presente entrevista.

Problema de investigación: En la era actual, los delitos informáticos están tomando fuerza debido a que las Tecnologías de la Información y la Comunicación se desarrollan de manera muy acelerada y de igual forma se van acoplando a este desarrollo los ciberdelincuentes que explotan estas nuevas tecnologías con el fin de realizar actos nocivos y dañinos para la ciudadanía y como es de conocimiento general, actualmente toda persona ya sea natural o jurídica, tiene como mínimo un dispositivo tecnológico en su hogar o en su lugar de trabajo, lo que los hace vulnerables a ser víctimas de estas acciones. Estos actos o conductas afectan ciertos bienes jurídicos como el patrimonio, la privacidad, la intimidad, etc. En Ecuador la tipificación de delitos informáticos ha sido algo ineficiente, por ende, es necesario realizar una comparación entre legislaciones para poder analizar y encontrar tipos penales que no están en nuestra legislación y así poder plantear una nueva reforma al Código Orgánico Integral Penal para sancionar nuevos ciberdelitos y de esta manera garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana.

ENTREVISTA

1. **En otras legislaciones a diferencia de Ecuador se tipifica y sanciona así: en el Código Penal de Costa Rica la estafa informática y la facilitación del delito informático. ¿Estima usted que la tipificación y sanción como delitos independientes de estas conductas en el Código Orgánico Integral Penal evitarían la impunidad?**

……
……
……
……

2. **¿Considera usted que para garantizar el ejercicio pleno de los derechos de la ciudadanía ecuatoriana debe tipificarse y sancionarse en el Código Orgánico Integral Penal como delitos independientes los siguientes: Estafa Informática, Facilitación del delito informático?**

……
……
……
……
……

3. **¿Está usted de acuerdo en Reformar el Código Orgánico Integral Penal tipificando y sancionando aquellas conductas que en la legislación penal extranjera constituyen delitos informáticos?**

……
……
……
……
……

4. **¿Considera usted que tipificando y sancionando las conductas descritas anteriormente se disminuiría el índice de la delincuencia que delinque utilizando medios informáticos?**

……
……
……
……
……

5. **¿Qué sugiere frente al problema planteado?**

……
……
……

Anexo 3. Certificado de Traducción Abstract

CERTIFICADO DE TRADUCCIÓN

Loja, 29 de noviembre de 2024

Yo, **Adriana Elizabeth Cango Patiño** con número de cedula 1103653133, Magister en Pedagogía de los Idiomas Nacionales y Extranjeros. Mención en Enseñanza de Inglés. **Registro Senescyt 1049-2022-2589539**

CERTIFICO:

Haber realizado la traducción de español al idioma inglés del resumen del trabajo de integración curricular denominado: **"Análisis Jurídico y Doctrinario de los Delitos Informáticos Tipificados en Colombia, Perú y Costa Rica para incorporarlos al Código Orgánico Integral Penal",** del señor **Gabriel Alejandro Cabrera Vivar con** número de cédula **1106046517,** estudiante de la Carrera de Derecho de la Facultad Jurídica, Social y Administrativa de la Universidad Nacional de Loja. Dicho estudio se encontró bajo la dirección del **Dr. Guilber René Hurtado Herrera, Mg. Sc**, previó a la obtención del título de Abogado. Es todo cuanto puedo certificar en honor a la verdad, y autorizo al interesado hacer uso del documento para los fines académicos correspondientes.

Atentamente,

Mg. Sc. Adriana Elizabeth Cango Patiño
Magister en Pedagogía de los Idiomas Nacionales y Extranjeros. Mención en Enseñanza de Inglés
Celular: 0989814921
Email: adrianacango@hotmail.com