



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL
FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

TEMA:

**Los delitos informáticos y los vacíos legales que afectan a
los ciudadanos**

AUTOR:

Chiluisa Mullo Dany Oswaldo

**Trabajo de titulación previo a la obtención del título de
Abogado de los tribunales y juzgados de la república del
Ecuador**

TUTORA:

Dra. Ángela María Paredes Cavedo

**Guayaquil – Ecuador
23 de febrero de 2021**



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y

POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Chiluisa Mullo Dany Oswaldo**, como requerimiento para la obtención del título de **Abogado de los Tribunales y Juzgados de la República del Ecuador**.

TUTORA

f. _____

Dra. Angela María Paredes Cavedo

DIRECTOR DE LA CARRERA

f. _____

Mgs. María Isabel Lynch Fernández

Guayaquil, a 23 días del mes de febrero de 2021



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Chiluisa Mullo Dany Oswaldo**

DECLARO QUE:

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

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

Guayaquil, a 23 días del mes de febrero de 2021

EL AUTOR

f. _____

Chiluisa Mullo Dany Oswaldo



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Chiluisa Mullo Dany Oswaldo**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la publicación en la biblioteca de la institución del Trabajo de Titulación: **Los delitos informáticos y los vacíos legales que afectan a los ciudadanos** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a 23 días del mes de febrero de 2021

EL AUTOR:

f. _____

Dany Oswaldo Chiluisa Mullo

REPORTE URKUND

TUTORA

f. _____

Dra. Angela María Paredes Cavedo

AUTOR

f. _____

Chiluisa Mullo Dany Oswaldo

AGRADECIMIENTO

La gratitud como una semilla que crece en suelo fértil es la mejor forma de demostrar el mas sincero reconocimiento a todas aquellas personas e instituciones que han permitido cristalizar un sueño. De manera especial, quiero agradecer a mi querida esposa María José por su constancia, paciencia y apoyo incondicional.

Así mismo, a mis queridos padres Oswaldo y Miriam por sus enseñanzas, ejemplo e infinito amor.

Como no, a mi querida Universidad Católica de Guayaquil por abrirme las puertas del saber, a mis docentes por su esmero y dedicación. De forma especial a mi tutora por su grata colaboración en la realización de este trabajo.

A todos ustedes.

Con infinita gratitud.

Dany

DEDICATORIA

Porque no basta la gratitud, con infinito cariño este trabajo de investigación se lo dedico mi amada María José y como no a mis adorados hijos Danny y Danna, la razón de mi vida y el motivo para luchar día a día, siendo su ejemplo y mas que su padre su amigo.

A ustedes querida familia se los dedico este grato esfuerzo.

Así también, a cada uno de futuros abogados, este trabajo servirá de guía para nuevas investigaciones que se planteen respecto del tema. Como futuros profesionales del derecho nuestro deber es buscar siempre la justicia.

A ustedes mis amigos.

Con infinita gratitud.

Dany



**UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL**

**FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES Y
POLITICAS**

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____
AB. MARIA ISABEL LYNCH DE NATH, MGS.
DECANO O DIRECTOR DE CARRERA

f. _____
AB. PAOLA TOSCANINI SEQUEIRA, MGS.
COORDINADOR DEL ÁREA O DOCENTE DE LA CARRERA

f. _____
AB. MARIA PAULA RAMIREZ VERA, MGS.
OPONENTE

ÍNDICE GENERAL DE CONTENIDOS

	Pág.
AGRADECIMIENTO	VI
DEDICATORIA	VII
ÍNDICE GENERAL DE CONTENIDOS	IX
RESUMEN EJECUTIVO	XI
ABSTRACT	xii
CAPÍTULO I	2
INTRODUCCIÓN	2
1.1. Tema de investigación	2
1.2. Planteamiento del problema	2
1.3. Pregunta de investigación	3
1.4. Antecedentes investigativos	3
1.5. Palabras clave y conceptos nucleares	4
1.6. Justificación	4
1.7. Objetivos	5
1.8. Metodología a ser empleada	5
CAPITULO II	8
MARCO TEÓRICO	8
2.1. Origen y evolución de los delitos informáticos	8
2.2. Derecho a la intimidad y protección jurídica de las personas	10
2.3. Vacíos jurídicos en el contexto normativo ecuatoriano	12
CAPÍTULO III	15
MARCO JURÍDICO	15
3.1. Delitos y criminalidad informática desde una perspectiva normativa	15

3.2. Conductas delictivas entorno a la clasificación de ilícitos informáticos.....	16
3.3. Delitos informáticos, tipificación y posibles anomias jurídicas...18	18
CONCLUSIONES	22
RECOMENDACIONES.....	23
REFERENCIAS BIBLIOGRÁFICAS	25

RESUMEN EJECUTIVO

El sistema jurídico ecuatoriano contiene un amplio andamiaje normativo a través del cual se garantiza la protección jurídica de las personas. Bajo este contexto, de forma simultánea se presenta también una serie de vacíos y contraposiciones normativas en razón de que los continuos avances jurídicos requieren fortalecer esfuerzos a fin de ir a la par de la evolución social y tecnológica. De modo que, el desarrollo tecnológico trae consigo una nueva corriente delictiva, la cual no se encuentra tipificada en su totalidad debido a la dificultad que implica su regulación al trascender fronteras. Por esta razón, el objetivo de este trabajo de investigación ha sido “elaborar un ensayo crítico jurídico en evidencia de los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación con los delitos informáticos que actualmente afectan a los ciudadanos”. Para el efecto, se cuenta con un sustento bibliográfico, doctrinario y legal preciso, mismo que dentro de un enfoque cualitativo se ha constituido en el principal soporte para la elaboración de este trabajo. Finalmente, luego de exponer la problemática actual que deriva de los vacíos jurídicos expuestos se contrasta la realidad social y normativa para posteriormente plantear posibles soluciones.

Palabras claves: anomias, delitos informáticos, tutela efectiva.

ABSTRACT

The Ecuadorian legal system contains a broad regulatory framework through which the legal protection of people is guaranteed. In this context, simultaneously there are also a series of regulatory gaps and contrapositions because the continuous legal advances require strengthening efforts in order to keep up with social and technological evolution. Thus, technological development brings with it a new criminal trend, which is not fully typified due to the difficulty involved in regulating it as it transcends borders. For this reason, the objective of this research work has been "to develop a critical legal essay in evidence of the existing legal gaps in the Ecuadorian legal system and that are related to computer crimes that currently affect citizens." For this purpose, there is a precise bibliographic, doctrinal and legal support, which within a qualitative approach has become the main support for the preparation of this work. Finally, after exposing the current problems that derive from the exposed legal gaps, the social and normative reality is contrasted to later propose possible solutions.

Keywords: anomies, computer crimes, effective guardianship.

CAPÍTULO I

INTRODUCCIÓN

1.1. Tema de investigación

Los delitos informáticos y los vacíos legales que afectan a los ciudadanos.

1.2. Planteamiento del problema

El ordenamiento jurídico ecuatoriano a través de sus diferentes preceptos normativos tiene como objetivo principal regular la convivencia y armonía social. Es por esta razón que mediante la integración de un cuerpo normativo actualmente denominado Código Orgánico Integral Penal (2014) se recoge y cataloga las diferentes infracciones que deben ser sancionadas por el poder punitivo. En estas infracciones se destacan delitos y contravenciones mismos que para ser castigados se aplica una pena proporcional al daño ocasionado, la cual va de acuerdo al nivel de gravedad producido. No obstante, la continua evolución social trajo consigo una novedosa corriente tecnológica que ha ido a su vez forjando una serie de ilícitos que por su naturaleza misma requieren un amplio estudio legislativo para su posterior tipificación.

La relevancia y novedad del tema expuesto resulta importante en razón de que, el Código Orgánico Integral Penal ecuatoriano instituye preceptos de forma general para la sanción de delitos informáticos, sin embargo, no se tipifica en razón de proporcionalidad cada uno de estos tipos penales ocasionando la existencia de anomias denominadas vacíos jurídicos. En este orden de ideas, es preciso resaltar que, ante la presencia de diversas actividades delictivas perpetradas mediante las estructuras electrónicas y tecnológicas, van ligadas una serie de herramientas delictivas enfocadas a alterar el orden social y manipuladas por delincuentes especializados en la violación de derechos informáticos. De modo que, la normativa existente en cuanto a la protección integral de las diferentes tecnologías de la información dificulta la prevención y sanción total de los delitos cometidos por cuanto estos componentes se estancan en lagunas jurídicas.

1.3. Pregunta de investigación

Para ser específicos y en razón de los argumentos establecidos, en el desarrollo de este estudio se pretende evidenciar: ¿De qué manera los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación a los delitos informativos afectan a los ciudadanos?

1.4. Antecedentes investigativos

Son varios los investigadores, estudiantes y tratadistas que abordan el tema que se ha expuesto en esta línea de investigación. Por esta razón, el sustento doctrinario que aportan es esencial para la consecución de los objetivos planteados. De modo que:

Chauca Acero (2014) en el estudio titulado “El principio de proporcionalidad en la prevención de los delitos informáticos”, en el texto se menciona que “El desconocimiento de los derechos y procedimientos a seguir legalmente en el caso de ser víctima del delito contra la intimidad o privacidad informática, limita las sanciones que se deben aplicar dentro del ámbito legal por la mala utilización de las redes sociales”. De este modo se analiza y sustenta la existencia de vacíos jurídicos en el marco del sistema legislativo ecuatoriano.

Riofrío Tacuri (2012) “Los Delitos Informáticos y su Tipificación en la Legislación Ecuatoriana” en este artículo el autor analizar varios puntos criminógenos que a su juicio “afectan a los bienes jurídicos de las personas” sostiene además que los mismos “no tienen su adecuación a un tipo penal establecido dentro del Código Penal”. De modo que, a través de un estudio comparado entre varias legislaciones de países de la región propone la adecuación unitiva de estas figuras jurídicas.

Ruiz Cruz, (2016) en su tema de investigación “Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos” expone el vertiginoso avance de las tecnologías de la información, así como la progresiva celeridad entorno a los delitos informáticos. Por tal razón, la investigadora argumenta la necesidad de

“tipificar y sancionar la apropiación ilícita de la información privada de las personas en las redes sociales”.

1.5. Palabras clave y conceptos nucleares

Anomias: a efectos de la interpretación normativa, las anomias constituyen vacíos o lagunas jurídicas en las que de acuerdo a la tradición sociológica se define como “ausencia permanente de normas” (Reyes Morris, 2008). Con esta definición se hace útil entender la naturaleza de las diferentes situaciones jurídicas que presentan constante conflicto normativo. El concepto en la actualidad tiene amplia injerencia y vinculación a los conceptos de delitos y criminalidad como se analiza en este contexto.

Delitos informáticos: son diferentes los conceptos que surgen a la luz de los delitos. Es por esta razón que tomando la definición de Téllez Valdés (1996) se establece que “delito informático en forma típica y atípica constituye una conducta antijurídica y culpable en la que se tiene a las computadoras como instrumento o fin”. Por otra parte, se manifiesta que son: “aquellas conductas que implican destrucción o inutilización de datos o programas de sistemas informáticos, que suelen ligarse con el sabotaje y el espionaje informático” a su vez “implican alteración o manipulación de datos o programas de sistemas informáticos” (Mayer Lux, 2017).

Tutela efectiva: básicamente se constituye como “el derecho de acudir al órgano jurisdiccional del Estado a fin de que el mismo disponga una respuesta fundada en derecho a una pretensión”. Este mecanismo se efectiviza al momento de reunir las condiciones mínimas como garantías fundamentales con las que cuentan los ciudadanos al momento de hacer efectivos sus derechos o a hacerlos justiciables ante sus transgresión (Aguirre Guzmán, 2010, pp. 14-15).

1.6. Justificación

Actualidad: Los diversos antecedentes históricos en cuanto a la evolución de los Delito Informático en el contexto jurídico ecuatoriano trae consigo una serie de conflictos normativos que se producen al momento de judicializar

diferentes eventos producto de los delitos informáticos. Al no encontrarse debidamente adecuados a la legislación interna surgen vacíos jurídicos que provocan transgresión de derechos. Por esta razón, la problemática planteada tomará en cuenta las diferentes particularidades a fin de constituir un novedoso y positivo impacto en la sociedad.

Importancia: el tema expuesto radica su importancia jurídica en razón de que el estado ecuatoriano tiene la obligatoriedad de establecer normas vigentes, claras y precisas para la protección de los derechos. En este sentido, al verificar la existencia de lagunas normativas el estado incumple con su rol de garante de derechos y permite que la ciudadanía no cuenta con la tutela efectiva que se le ofrece al tenor del texto constitucional como norma jerárquicamente aplicable. De ahí deriva la necesidad de exponer este texto académico analizando y determinando una necesidad jurídica en el contexto actual.

1.7. Objetivos

a. Objetivo general

- ✓ Elaborar un ensayo crítico jurídico en evidencia de los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación con los delitos informáticos que actualmente afectan a los ciudadanos.

b. Objetivos específicos

- ✓ Describir desde un punto de vista teórico los diferentes elementos y conceptos doctrinarios para esclarecer el conocimiento y la evolución de los delitos informáticos en el Ecuador.
- ✓ Exponer la incidencia de los delitos informáticos entorno a la aplicación de la normativa jurídica ecuatoriana a fin de determinar el grado de seguridad jurídica al momento de prevenir y tipificar delitos.

1.8. Metodología para emplear

Basados en el tipo de investigación descriptiva, para el desarrollo sistemático de este contexto el investigador se respalda en el uso del método teórico de

reseña o revisión, mismo que a través de un estudio analítico sintético permite examinar estudios previos y antecedentes en cuanto al análisis de delitos informáticos. Al descomponer los fenómenos y modelos jurídicos de estudio en sus partes se las examina dejando en evidencia criterios argumentativos y la postura del autor de forma individual. Una vez realizado este paso se procede a la integración de ideas, propuestas y preceptos que han servido para nutrir la investigación científica. Se debe resaltar la importancia del uso y aplicación de estos métodos en razón de que los mismos permite ir de lo general a lo particular y viceversa.

La metodología que se usa dentro del área social por su naturaleza misma tiene un enfoque cualitativo, por medio del cual se expone de las diferentes fuentes de consulta como técnica de investigación las cuales se adentran en un estudio bibliográfica, documental, exploratorio y descriptivo. Por medio de estos mecanismos y métodos expuestos se profundiza en las ideas presentadas a fin de cumplir con los objetivos propuestos.

Instrumentos de investigación: a la luz de las categorías de análisis descritas se procede a realizar una investigación descriptiva y cualitativa con el propósito de profundizar la realidad ecuatoriana actual.

Análisis e interpretación: de forma concreta los datos teóricos, doctrinarios y legales sirven para consolidar resultados y fundamentar el artículo académico que se expone. La investigación tiene un soporte doctrinario, legal y fundamental mismo que permite exponer de forma clara el tema expuesto. Asimismo, durante el desarrollo de los capítulos el autor analiza de forma concreta la realidad actual basado en el soporte expuesto mediante los resultados obtenidos en la investigación.

1.9. Categorías de análisis

El desarrollo del presente ensayo contiene dos capítulos mismos que se abordan desde un andamiaje doctrinario y jurídico. Por esta razón, el contenido categórico de la información responde a:

Marco teórico:

- ✓ Origen y evolución de los delitos informáticos
- ✓ Derecho a la intimidad y protección jurídica de las personas
- ✓ Vacíos jurídicos en el contexto normativo ecuatoriano

Marco jurídico:

- ✓ Delitos y criminalidad informática desde una perspectiva normativa
- ✓ Conductas delictivas entorno a la clasificación de ilícitos informáticos
- ✓ Delitos informáticos, tipificación y posibles anomias jurídicas

Discusión y resultados

Finalmente, se expone los resultados obtenidos dentro del proceso investigativo que se presenta, para lo cual se cuenta con el sustento y análisis de la metodología propuesta y las opiniones de expertos en la materia. Por tanto, se expone las conclusiones y recomendaciones que el estudiante ha obtenido en razón de la presente investigación. En las conclusiones, el autor se manifiesta de forma clara, precisa y con el respectivo sustento investigativo la necesidad de una reforma a la norma penal. Asimismo, las recomendaciones que se abordan surgen a consecuencia de los preceptos investigados y puestos a consideración de la academia. Con este trabajo investigativo, el estudiante aporta de forma significativa a la investigación con un trabajo que servirá de precedente para próximas investigaciones que se encaminen y se sustenten respecto del tema en particular.

CAPITULO II

MARCO TEÓRICO

2.1. Origen y evolución de los delitos informáticos

La constante evolución y el uso de herramientas tecnológicas han facilitado el desenvolvimiento personal tanto en el ámbito profesional, educativo académico, comunicativo, laboral, cultural social, entre otros. Si bien, el uso de la tecnología ha generado grandes avances para la ciencia, a la par ha evolucionado también los efectos negativos por el mal uso de esta herramienta. La influencia tecnológica se hace presente en todas las ramas del conocimiento, así como en la vida diaria de las personas. Esto se hace útil para ahorrar tiempo y dinero en tramites o procedimientos que años atrás acarrearón una excesiva tardanza. Para nadie es desconocido que esta revolución tecnológica trajo consigo avances para la vida moderna, no obstante, su eficacia siempre estará supedita a la aplicación y regulación normativa como base hegemónica en la convivencia humana.

La globalización actual ha desarrollado una nueva forma de delincuencia que difieren ampliamente de la común, sin embargo, en razón de su contenido ilícito conserva sus rasgos de culpabilidad e inexorablemente debe ser sancionado. Es así que un delito informático regularmente es cometido por sujetos con habilidades cognoscitivas y estrategias específicas. En contraste a esta afirmación Encalada (2010, p. 23) sostiene que “el nivel típico de aptitudes del delincuente informático es tema de controversia” y añade que en ocasiones “el nivel de aptitudes no es indicador de delincuencia informática”. Sin embargo, el delincuente informático habitualmente debe ser una persona muy lista y con aptitudes tecnológicas. Sin embargo, dejando de lado el análisis del sujeto cabe cuestionar la dificultad para sancionar estos actos por cuanto no siempre víctima y agresor están sujetos a normativas jurídicas análogas.

Para definir un delito informático se puede recurrir a diferentes conceptos doctrinarios, así Pérez Luño manifiesta que es “aquel conjunto de conductas

criminales que se realizan a través de un ordenador electrónico o que afectan al funcionamiento de los sistemas informáticos” (1996, p. 18). Estos comportamientos delictivos en la actualidad no siempre requieren de una computadora, los celulares son un mecanismo bastante accesible para los nuevos ilícitos, ya que las redes sociales son bastantes franqueables y exponen de forma amplia la interacción de las personas. Para complementar lo establecido, los componentes de una red social son: “a. actores, que pueden ser individuales o colectivos b. lazos, la relación o vínculo entre ellos c. vinculación, medio de interacción entre los actores” (Rodríguez, 2018, p. 18).

Para complementar lo descrito, la norma jurídica ecuatoriana sanciona algunos de estos delitos como se verá más adelante, sin embargo, en la contextualización expuesta se ha hecho necesario recurrir a la doctrina para consolidar la teoría conceptual que gira entorno a estos ilícitos. Así, se ha podido precisar que al hablar de delitos informáticos, estos se constituyen en dos tipos, “los delitos computacionales y delitos informáticos propiamente dichos” (Riofrío Tacuri, 2012, p. 17). Entonces, lo que los diferencia entre unos es que la conducta delictiva de los primeros tiene como fin la afectación del patrimonio de las personas, lo que incluye: bienes, cuentas, derecho a la intimidad y hasta la seguridad pública. Mientras que, en los segundos, el ataque y daño es perpetrado entre sí, es decir el ataque al software permite una intromisión, acceso a computadoras, datos y registros.

Para simplificar lo expuesto y siguiendo la línea del pensamiento de Zabala Baquerizo,

“(…) la gran diferencia entre delito informático y computacional, el primero que es un atentado al soporte lógico de un sistema de procesamiento de información, en cambio el segundo, por medio de los sistemas informáticos se vulneran bienes jurídicos reconocidos penalmente como delitos contra la persona, contra el honor, la libertad, la seguridad pública o de la nación” (2015, p. 32).

Por otra parte, la persona que comete estos ilícitos es denominada ciber delincuente, mismos que pueden ser Hackers o Cracker. El Hacker, invade los sistemas operativos como un reto intelectual, demuestra su potencial, crea

software, quebranta seguridades, pero todo esto sin fines económicos. Mientras que los Cracker, tienen como propósito generar daño de forma intencional buscando su beneficio personal. Una de las variantes de estos actores delictivos son los piratas informáticos que al perpetrar en los diferentes sistemas: producen daños, desprotegen programas, roban información, entre otros ilícitos. El mundo informático es tan amplio que delimitar cada uno de los delitos resulta en un verdadero reto, así Villalobos estudia al sujeto activo desde sus diferentes características que de acuerdo al ataque realizado, a más de los Hackers y Cracker también pueden ser: “Trashing o Mercenarios y traficantes de la información, Terroristas y Grupos extremistas, Phreaker o cracker telefónico, Lammers, Gurus, Bucaneros: Newbie”. Mientras que, como sujeto pasivo se está la víctima de todos estos ilícitos (2012, pp. 53-59).

2.2. Derecho a la intimidad y protección jurídica de las personas

Ahora bien, una vez que se ha establecido de forma concreta el delito informático, sus características, actores y precedentes, es menester examinar los derechos de la víctima entorno a su trasgresión. Bajo este contexto, sabiendo que los derechos consagrados en la Constitución y en los instrumentos internacionales, como lo analiza Cáceres (2020) son de directo e inmediato cumplimiento, se hace necesario determinar que los derechos son históricamente prerrogativas concedidas en favor de los ciudadanos como mecanismos de frenos al poder y a la arbitrariedad. Así, en uso de los derechos estos por su naturaleza pueden ser humanos, fundamentales y constitucionales; mismos que en un estado de derechos como lo es el Ecuador convergen en una transversalidad otorgando su titularidad en igualdad de condiciones a todos los habitantes del territorio sin ningún tipo de discriminación.

Por lo tanto, la intimidad personal se convierte en un eje de la dignidad humana, que como lo señala De Sousa Santos “es el lenguaje hegemónico del respeto a los derechos humanos” (2014, p. 25). De modo que, la intimidad personal y familiar de las personas se encuentra reconocido en el numeral veinte del artículo 66 del texto constitución vigente, mismos que trata de los derechos de libertad. Es así, que este derecho humano y fundamental, dentro

del constitucionalismo ecuatoriano se encuentra plenamente reconocido. De tal virtud deriva la protección jurídica y normativa como facultad para exigir la autonomía y protección en el ámbito personalísimo. Sin embargo, poco se dice acerca del contenido del derecho a la intimidad, para ello el jurista argentino Nino (2007) al hacer referencia a la intimidad afirma que este derecho contiene inmerso varios aspectos, así: “rasgos del cuerpo, imagen, pensamientos, emociones” así también hechos relativos a su vida personal tales como: “conductas, grabaciones conversaciones, correspondencia, domicilio, situación económica, etc.” (p 328).

Por tanto, la privacidad, así como la intimidad personal desde su ámbito de protección jurídica en situaciones diversas se encuentra desprovisto. Así, por ejemplo, a través de las diferentes páginas de uso y dominio publico como son las que brindan servicios las propias instituciones del Estado como: Consejo de la Judicatura (SUPA, E-SATJE), IESS, SRI, ANT, SENESCYT, entre otras páginas en las que se visibiliza de forma pública datos personales con el solo hecho de conocer apellidos o cédulas de personas de las que se desea conocer información. Si bien es cierto, en propio ordenamiento jurídico ecuatoriano a través de la Ley Orgánica de Transparencia y acceso a la información publica ha instaurado estos mecanismos de consulta, a su vez también es un arma de doble filo que pone en entredicho la intimidad personal. Por cuanto, el pasado judicial, las deudas en firme o cualquier otro dato de acceso público puede ser motivo de discriminación que pone en situación vulnerable a los ciudadanos.

Llegado a este punto, resulta adecuado aceptar la diferenciación entre privacidad e intimidad, en tanto que la intimidad como lo sugiere Pérez Royo resulta ser un concepto democrático toda vez que deriva en un asunto complicado definirlo con precisión. De manera que, el derecho a la intimidad muy distinto del derecho al honor, consiste en poder disfrutar de forma única, situaciones personales en las que es preciso excluir a los demás como exigencia cultural que deriva de la dignidad humana (2002, p. 395). Al ser la intimidad un derecho personalísimo e innato del ser humano se convierte en un derecho subjetivo, por consiguiente, los derechos de personalidad también

han sido positivados en la Declaración Universal de Derechos Humanos a inicios del siglo XX. Este instrumento internacional en su artículo 12 consagra que “nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección jurídica de la ley contra tales injerencias o ataques” (1948).

Por lo expuesto, deriva la necesidad de protección jurídica de la intimidad personal por cuanto el derecho ha sido eco nacido ya desde un ámbito internacional y consolidado en el constitucionalismo ecuatoriano. Se debe recordar que la norma suprema vigente posiciona los instrumentos internacionales en una categoría jerárquica igual a la suya. No obstante, como se viene reiterando los avances tecnológicos obligan a consolidar nuevos mecanismos y sistemas de protección no únicamente desde el plano técnico y material sino también desde un aspecto jurídico muy necesario para subsanar los diferentes vacíos jurídicos que giran entorno a este problema de actualidad. Por esta razón, no basta conocer el contenido y la dimensión subjetiva de un derecho, es necesario ir más allá y posicionarse en la realidad social, lo cual es labor del legislador la creación de normas que regulen de forma adecuada la convivencia en sociedad.

2.3. Vacíos jurídicos en el contexto normativo ecuatoriano

Interesante resulta ir analizando cada uno de estos problemas sociales que como se ha detallado a lo largo del texto, derivan del propio ordenamiento jurídico. Por consiguiente, al hablar de delitos necesariamente debe existir: el sujeto activo, la víctima y por consiguiente el bien jurídico protegido. En este ámbito se puede destacar: “a. El patrimonio. b. La reserva, la intimidad y confidencialidad de los datos. c. La seguridad o fiabilidad del tráfico jurídico o probatorio. d. El derecho de propiedad” (Rodríguez, 2018, p. 33).

El Código Orgánico Integral Penal, pese a ser una norma relativamente nueva no prevé respuestas que sean validas de forma coherente a la actual delincuencia informática. En base a lo establecido, se puede argumentar que el contenido normativo penal requiere reformas que incluyan este nuevo

modelo de delitos y castiguen los mismos de forma particular. Como se viene analizando, una norma sancionatoria no contribuye a la prevención del delito, pero si a su reglamentación y disminución. El derecho informático al ser bastante amplio requiere una adecuada intervención de la norma penal para tipificar ciertos actos. Por ejemplo, en la actualidad se escucha sobre recurrentes fraudes electrónicos de los que generalmente las víctimas son clientes de cualquier institución bancaria en las que sin tener conocimiento sus dineros ya fueron utilizados por terceros.

De este modo, las denominadas estafas con tarjetas de crédito, transferencias bancarias no autorizadas, escaneo de puertos y siendo más pragmáticos el uso de wifi de cualquier lugar por medio de programas o forma de desmontar claves. Son entre otros los delitos que están en boga en los últimos meses. El problema va más allá, por cuanto las víctimas no tienen seguridad jurídica para recurrir a la autoridad competente a denunciar, ya que el ilícito no está configurado dentro de ningún tipo penal. Al respecto, el Código Orgánico Integral Penal en su artículo 190 detalla:

Artículo 190. Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Siendo este precepto legal bastante amplio y ambiguo es el único aplicable para sancionar algunos de los delitos informáticos, entre los que se detallaba los ocurridos con las cuentas bancarias de los clientes de los bancos que actualmente son víctimas. Asimismo, respecto del tema los delitos informáticos, estos se distinguen por poseer una naturaleza totalmente distinta en cuanto a la protección del bien jurídico que ostentan los delitos

tradicionales. La interrelación de las personas en sociedad se caracteriza por poseer distintos fines, entre ellos políticos, económicos entre otros. Son justamente estos fines y con mayor énfasis los fines económicos los que permiten configurar estafas y otros medios fraudulentos de apropiación de bienes. Por esta razón es importante, que en la legislación vigente se instituya las nuevas formas de estafa y fraude electrónico para que se garantice el patrimonio de las personas.

CAPÍTULO III

MARCO JURÍDICO

3.1. Delitos y criminalidad informática desde una perspectiva normativa

A la hora de regular los diferentes tipos penales, el legislador acentúa diferentes tipos de orientación dependiendo del lugar en donde estos se desarrollen. Así, al ser la criminalidad informática un tema bastante nuevo y controversial, sus preceptos sancionatorios aparecen desde hace menos de cincuenta años. Es así que, en los diferentes marcos jurídicos extranjeros, para ser específicos Estados Unidos y Europa sancionan por primera vez los abusos a los sistemas informáticos que en la actualidad se denominan virus informáticos. Es así que, desde una perspectiva internacional la Organización de las Naciones Unidas (ONU) en conjunto con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) han sido entes promotores al momento de definir y clasificar estos delitos y luchar en contra de la delincuencia informática.

Los actos antijurídicos y culpables en la legislación ecuatoriana se los conoce como infracciones de las que derivan los delitos y contravenciones. Con la promulgación de la norma penal ecuatoriana conocida como COIP “Código Orgánico Integral Penal” vigente desde 2014 se consolidó el derecho objetivo y subjetivo en materia penal, tipificando y sanciona algunos elementos delictivos en los que para su cometimiento se recurre al uso de medios informáticos. Así, considerando que el ciberespacio se ha convertido en el principal escenario para expandir la delincuencia informática traspasando fronteras y convirtiendo a estos ilícitos en motivo de inquietud nacional y mundial. Enfrentar delitos informativos se ha convertido en un verdadero reto en la actualidad por cuanto la constante evolución tecnológica impide pormenorizar cada de uno de los delitos exhibiendo así carencia de normas y vacíos jurídicos.

Haciendo un recorrido de lo general a lo particular, cabe abordar la creación de la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos (2002) ha promovido en la población la necesidad de acceso a servicios

electrónicos como un medio para el desarrollo de la educación y cultura. De este modo es como se ha intentado garantizar la protección de datos personales infundiendo los derechos de privacidad, intimidad y confidencialidad. Siendo uno de los mayores deberes y responsabilidades del estado la protección jurídica y la tutela efectiva de los derechos, cabe cuestionarse si entorno a la perspectiva normativa existente, si esta es necesaria para salvaguardar derechos o a su vez falta mucho por hacer y aún estamos frente a la existencia de vacíos normativos al momento de enfrentarnos a la criminalidad informática. No se conoce con precisión las cifras de los delitos informáticos cometidos en el Ecuador ya que al momento de su observación estas resultan un poco inciertas por cuanto no todas estas tipificadas y a su vez las víctimas no siempre ingresan la denuncia pertinente.

3.2. Conductas delictivas entorno a la clasificación de ilícitos informáticos

Son múltiples las clasificaciones que al respecto se han podido obtener, el investigador Acurio del Pino señala: “fraudes, sabotaje informático, espionaje hurto o robo de software, acceso no autorizado a redes y servicios”. Mientras tanto, de acuerdo a la clasificación de Cea Jiménez los delitos en redes sociales se relacionan con “acceso, adquisición, manipulación y divulgación de información” (citado en Rodríguez, 2018). Por consiguiente, allanar y apoderarse de información ajena constituyen diferentes mecanismos para configurar “estafas, modificación de datos, destrucción o apropiación de información, propagación de virus”. A consecuencia de la divulgación de información de forma conexa se vinculan otros delitos como: pornografía infantil, acoso sexual, amenazas, chantajes, extorsiones, divulgación de asuntos confidenciales, piratería entre otros delitos.

Por tanto, siendo tan amplia la clasificación delictiva, esta diversidad en cuanto a las conductas ilícitas e informáticas afectan de forma primigenia a toda la sociedad. De modo que, para la configuración del ilícito coadyuvan varias conductas entre las que se puede destacar: “la imaginación del autor, su capacidad técnica y las deficiencias del control existentes en las instalaciones informáticas” (Camacho Losa, citado en Rodríguez, 2018). En

razón de ser múltiples las conductas delictivas, la clasificación de estos ilícitos informáticos se debería realizar de forma oportuna en el contexto jurídico nacional como un mecanismo para contrarrestar la impunidad de estas conductas tipificándolas en ciertas leyes. Para precautelar la defensa de derechos de los usuarios informáticos la constitución ecuatoriana reconoce y garantiza “el derecho a la intimidad personal y familiar” así como “el acceso universal a las tecnologías de información y comunicación” (artículo 66 numerales 2 y 20).

En cuanto a la clasificación de los delitos informáticos se tomará como referencia la propuesta por el catedrático ecuatoriano en derecho penal informático Acurio del Pino (2015) mismo que establece:

“1. Fraudes:

Los datos falsos engañosos
Manipulación de programas
Técnicas de salami
Falsificaciones Informáticas
Manipulación de datos de salida
Clonación de tarjetas de crédito
Clonación de tarjetas de débito
Pishing

2. Sabotaje informático:

Bombas lógicas
Gusano informático
Virus informático y malware
Ciberterrorismo
Ataques de denegación de servicio
Las redes robot.

3. El espionaje informático y robo o hurto de software

Fuga de datos
Reproducción no autorizada de programas informáticos

4. El robo de servicios:

Hurto de tiempo del computador
Apropiación de informaciones residuales

Parásitos informáticos

5. Acceso no autorizado a sistemas informáticos:

Las puertas falsas
La llave maestra
Pinchado de líneas
Piratas Informáticos”

Por consiguiente, una vez establecido de forma pragmática cada uno de los elementos y componentes de las conductas delictivas, así como la

clasificación de los delitos informáticos es preciso pasar a un análisis pormenorizado de los tipos penales que destaca la norma jurídica penal vigente, así como los elementos que aun no constan en el catálogo de protección de derechos.

3.3. Delitos informáticos, tipificación y posibles anomias jurídicas

En el Código penal vigente (COIP, 2014) tipifica varios delitos relacionados con el uso de la tecnología. Así, al tenor del artículo 234 se menciona que “el acceso no consentido a un sistema informático, telemático o de telecomunicaciones” en contra de la voluntad de su legítimo titular con el fin de explotar, modificar, desviar datos o acceder a servicios evitando el pago a sus proveedores será sancionado con tres a cinco años de privación de libertad. La amenaza y la calumnia también son figuras jurídicas sujetas a sanción penal, sin embargo, juzgar estos ilícitos cuando la infracción se da por medio de redes sociales resulta un asunto bastante complejo debido a que la norma jurídica penal no está orientada a este contexto. Por otra parte, en cuanto al denominado “child grooming” que se traduce como “acoso sexual a menores mediante el uso del internet” (Puyol, 2019) es un tema bastante novedoso; sin embargo en la actualidad esta situación tampoco se encuentra regularizada de forma concreta.

En tanto, que el artículo 173 del COIP hace relación a este ilícito al sancionar “el contacto con finalidad sexual con menores de dieciocho años por medios electrónicos”. El uso de la fuerza, la intimidación, la coacción y hasta la violencia han sido los principales factores para configurar el cometimiento de estos delitos. En este aspecto se puede mencionar posibles embaucamientos y engaños a menores de edad de acuerdo al artículo citado, ya que la víctima se confía de la identidad que se visualiza y expone. En cuanto a la falsa identidad, a través de las redes sociales se hace más factible el fraude, así por ejemplo publicidad engañosa, que con identidad falsa o bajo el propio anonimato permite estafar masivamente al ofrecer productos y servicios de forma falaz. La estafa se sanciona con tres a cinco años de privación de libertad conforme lo expone el artículo 186, sin embargo, bajo el anonimato y sin pruebas suficientes esta figura resulta ineficaz para delitos cibernéticos.

Otro delito, no muy común en Ecuador, pero si usual en otros países es también el terrorismo y su financiación, ya que la tecnología actual insta para su perpetración. El racismo, la xenofobia la incitación al odio, la discriminación se palpa a diario en las redes sociales. La sanción que establece la norma penal se relaciona con los delitos de discriminación y actos de odio detallados en los artículos 176 y 177 del COIP. Sin embargo, existe el derecho a la libertad de expresión que está consagrado en la norma suprema que es la Constitución, por tal razón se hace necesaria la regulación normativa que evite ambigüedad y discrepancia entorno a la protección de los derechos de unos y otros. En cuanto a la violación de la intimidad el artículo 178 de la norma ibidem la sanción es de uno a tres años de prisión siempre y cuando se “acceda, intercepte, grabe, reproduzca, difunda información privada”.

Son reiteradas las situaciones que han puesto en evidencia la intimidad personal de varios ciudadanos en los que “reenviar” y difundir los mensajes, videos y fotos toma cuestión de segundos viralizando situaciones aparentemente jocosas en las que no existe un mínimo de respeto y empatía hacia sus protagonistas que en este caso podrían llamarse víctimas. Así, de manera momentánea circula información íntima, que por distintos eventos ridiculizan a sus actores y gran parte de la población hace apología y burla de la información recibida. No está por demás mencionar algunos casos que hasta reciben epítetos propios, por ejemplo: la muy señora, la jueza ebria, Julissa, como los mas mencionados a nivel nacional. De no haber vacíos normativos se hubieren tomado acciones legales en contra de quien violó su intimidad viralizando situaciones muy íntimas y atentando a la intimidad personal.

Otros de los delitos conocidos en el contexto normativo es el cyber-bullying a través del cual se consigue “agredir psicológicamente a uno o varias personas de forma repetitiva en el tiempo”. Esta figura se sanciona como falta muy grave constante en el Reglamento a la Ley Orgánica de Educación Intercultural. el cyber-bullying como tal está posicionado en el artículo 15 de la “Ley Orgánica de Prevención, Control y Sanción del Acoso, Intimidación o Violencia en los Centros de Estudio de Ecuador” expedida en el año 2013. Esta conducta

necesariamente para que se configure como tal se debe efectuar entre menores de edad. Si las características son similares y los actores son mayores de edad estamos frente a un cyber-stalking denominado Ciberacoso (Rodríguez, 2018, p. 23).

Para no hacer demasiado extensiva esta investigación, se concretará refiriendo al Pharming, Phishing, Sexting. La primera hace relación al ataque de paginas web con lo cual se obtiene información confidencial con fines fraudulentos. El Phishing, ocurre cuando la víctima es engañada e inducida por medio de suplantación a proporcionar información, los delincuentes suplantando la figura de entidades legales y engañan a su víctima. Finalmente, el Sexting se relaciona con el envío de contenido sexual cuando se difunde sin autorización. Como se ha podido destacar ninguno de estos delitos están tipificados en el actual cuerpo legal ecuatoriano. Es así como se ha evidenciado que normas están reguladas y cuales no en el contexto penal normativo, de modo que resta mucho por hacer a fin de garantizar y proteger derechos de forma adecuada e el marco jurídico ecuatoriano vigente.

El artículo 234 de la norma penal tipifica el “Acceso no consentido a un sistema informático, telemático o de telecomunicaciones” (COIP, 2014) en este precepto se sostiene que si el ingreso se realiza en contra de la voluntad del legítimo propietario del derecho con el fin de “a explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos” el responsable del ilícito será sancionado con pena privativa de la libertad de tres a cinco años. Asimismo, el ataque a la integridad de sistemas informáticos tipificado en el artículo 232 hace mención a una pena similar cuando:

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen. (COIP, 2014).

La revelación ilegal de base de datos en provecho propio o de un tercero articulada en el texto penal al tenor del precepto 229 impone una pena de tres a cinco años al igual que los casos anteriores. Otra de las figuras delictivas que se encuentran penadas es la interceptación ilegal de datos que sanciona a quien “intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático” (COIP, artículo 230). En teoría las sanciones representan una forma de prever los delitos, sin embargo, en la práctica a diario somos víctimas de la violación a la privacidad y la exposición de nuestros datos. No es novedad recibir llamadas de números desconocidos que de forma concreta conocen nuestros datos personales y llaman ofreciendo productos y servicios. Todas estas situaciones descritas en el texto perturban la tranquilidad de los ciudadanos y nos dejan en la indefensión jurídico al no existir parámetros que limiten estas actuaciones negativas.

CONCLUSIONES

Actualmente existe amplia diversidad entorno a la ejecución de la delincuencia informática, misma que ha ido trascendiendo fronteras a pasos agigantados dejando en la indefensión a miles de personas en razón de que se vulnera de forma constante su derecho a la intimidad. Siendo la intimidad un derecho humano protegido desde un ámbito histórico e internacional su esencia jurídica requiere ser reforzada a fin de que la evolución tecnológica vaya de la mano con el desarrollo jurídico que se requiere. Sin dejar de lado que el derecho al igual que la tecnología se encuentra en constante evolución y por su intermedio se debe dar respuestas oportunas a la sociedad al contener la normativa legal reglas de convivencia.

En el Ecuador, la reforma a la legislación penal y la vigencia del Código Orgánico Integral Penal, trae consigo una serie de cambios en cuanto a los procedimientos y la tipificación de nuevos delitos. No obstante, poco se dice respecto de las nuevas formas de delinquir que vienen ligadas a los delitos informáticos. Se debe tener en cuenta que, la tecnología se encuentra constantemente vinculada al desenvolvimiento social creando una necesidad de tipificación para nuevos delitos. Debido a que, la mayor parte de la población maneja y usa la tecnología, y es justamente por medio de las redes informáticas que se vuelve vulnerable la información que cada una de las personas confiere o comparte en las plataformas electrónicas.

El uso fraudulento de los sistemas informáticos deja en la indefensión a miles de personas, ya sean naturales o jurídicas puesto que los sistemas informáticos son altamente franqueables. De modo que, el funcionamiento de las redes electrónicas es totalmente manipulable por personas profesionales en el área que pueden fácilmente romper seguridades. Por tanto, la delincuencia común ha trascendido en un nuevo tipo de delincuencia organizada que usa la tecnología para beneficio y lucro propio. La mayor parte de delitos de esta naturaleza quedan en la impunidad al no haber un procedimiento adecuado para prevenir su comisión.

RECOMENDACIONES

De acuerdo a lo anotado en el texto, son diferentes las modalidades de delitos informáticos que se pueden cometer mediante el uso de la tecnología. Por consiguiente, es preciso resaltar que en la legislación Ecuatorina se hace urgente y necesario la reforma a la normativa penal a fin de sancionar de forma drástica los ilícitos que se vienen detallando, mismos que debido a vacíos jurídicos existentes quedan en la impunidad. Asimismo, respecto de la reforma normativa el legislativo debe contemplar esta posibilidad no solo en el texto penal sino también creando una ley que persiga y sancione los delitos informáticos. Se recomienda también, implementar mecanismos de protección por medio de una amplia revisión a la Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital vigente.

A fin de prevenir estos delitos informáticos, independientemente de la naturaleza de los mismos, en la legislación ecuatoriana se hace necesario que se regule el correcto funcionamiento de los sistemas informáticos por medio de la urgente intervención gubernamental que establezca políticas públicas de lucha contra la delincuencia informática. Para ello, se hace necesaria la intervención y cooperación internacional con otros países que instituyan y compartan sus experiencias en la lucha contra esta delincuencia. Por tanto, mediante esta regulación se puede implementar un procedimiento exclusivo con rigurosos mecanismos y profesionales con conocimientos técnicos en el área para perseguir y sancionar la delincuencia informática. Por esta razón se hace menester la suscripción de convenios y tratados internacionales.

Finalmente, también se requiere una oportuna capacitación a los operadores de justicia para que desde el contexto judicial se pueda capacitar por medio de profesionales en el área el manejo de la informática legal y forense mediante la cooperación de organismos especializados para el juzgamiento de estos ilícitos. a su vez, es una corresponsabilidad ciudadana la prevención de la delincuencia informática, por tal razón es preciso capacitar constante a toda la ciudadanía a fin de concientizar el uso seguro de las herramientas informáticas a fin de evitar que se conviertan en víctimas. Estas socializaciones también son responsabilidad estatal por medio de sus

instituciones para prevenir y advertir a todos los usuarios de sistemas informáticos un uso responsable de la tecnología.

REFERENCIAS BIBLIOGRÁFICAS

- Acurio del Pino, S. (2015). *Derecho Penal Informatico*. Corporación de Estudios y Publicaciones.
- Aguirre Guzmán, V. (2010). *La tutela judicial efectiva como derecho humano: Una aproximación a su concepción y situación en el Ecuador*. Universidad Andina Simón Bolívar.
- Asamblea Nacional . (2014). *Código Orgánico Integral Penal*. Quito: Registro Oficial 180 de 10 de febrero de 2014.
- Cáceres, N. (2020). *El principio de aplicación directa de la constitución y el control concreto de constitucionalidad en el Ecuador* [Tesis de Maestría]. Universidad Técnica de Ambato.
- Carrión, J. L. (2020). DELITO Y LA PENA. *DerechoEcuador.com*, 1.
- Chauca Acero, G. (2014). *El principio de proporcionalidad en la prevención de los delitos informáticos*. Universidad Autónoma de los Andes.
- Congreso Nacional. (2002). *Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos*. Registro Oficial Suplemento 557.
- De Sousa Santos, B. (2014). *Derechos humanos: Espejismos y desafíos*. En *Derechos humanos, democracia y desarrollo*. Ediciones Antropos.
- Encalada, G. (2010). *La criminalidad informática: Propuesta para la tipificación de los delitos informáticos en la legislación ecuatoriana*. Universidad de Cuenca.
- Jiménez de Asúa, L. (1997). *Principios de Derecho Penal—La Ley y el Delito* (tercera). Sudamericana S.A.
- Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, 44(1), 261-285. <https://doi.org/10.4067/S0718-34372017000100011>

- Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*.
https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf
- NINO, C. S. (2007). *Ética y Derechos Humanos—Un ensayo de fundamentación*. Astrea.
- Pérez Luño, A. (1996). *Manual de Informática y derecho*. Editorial Ariel.
- Pérez Royo, J. (2002). *Curso de derecho constitucional*. Marcial Pons.
- Puyol, J. (2019). *¿En qué consiste el «child grooming» [acoso sexual de menores por Internet] y qué medidas de prevención deben adoptarse?* Confilegal.
<https://confilegal.com/20190128-en-que-consiste-el-child-grooming-acoso-sexual-de-menores-por-internet-y-que-medidas-de-prevencion-deben-adoptarse/>
- Reyes Morris, V. (2008). Anomia y criminalidad: Un recorrido a través del desarrollo conceptual del término Anomia. *Revista Criminalidad*, 50(1), 319-332.
- Riofrío Tacuri, J. F. (2012). Los Delitos Informáticos y su Tipificación en la Legislación Ecuatoriana. *Universidad Nacional de Loja*, 201.
- Rodríguez, C. (2018). *Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador, determinación de vacíos legales y el proceso para propuesta de ley*. Universidad Internacional SEK.
- Ruiz Cruz, C. (2016). *Análisis de los delitos informáticos y su violación de los derechos constitucionales de los ciudadanos*. Universidad Nacional de Loja.
- Téllez Valdés, J. (1996). *Derecho Informático*. México D.F.: Mc Graw Hill.
- Vázquez, A. R. (2018). Investigadora describe perfil psicosocial de sicarios mexicanos. *Red Universitaria de Jalisco*, 1.
- Villalobos, E. (2012). *Diccionario de derecho informático*. Dykinson.
- Zabala Baquerizo, J. (2015). *Delitos Informáticos en el Ecuador*. Edino.



**Presidencia
de la República
del Ecuador**



**Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes**



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

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Dany Oswaldo Chiluisa Mullo**, con C.C: **0502682032** autor del trabajo de titulación: **Los delitos informáticos y los vacíos legales que afectan a los ciudadanos**, previo a la obtención del título de **abogado de los tribunales y juzgados de la república del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

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

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

Guayaquil, 23 de febrero del 2021

f. _____

Chiluisa Mullo Dany Oswaldo

C.C: 0502682032



Presidencia
de la República
del Ecuador



Plan Nacional
de Ciencia, Tecnología,
Innovación y Saberes



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

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	Los delitos informáticos y los vacíos legales que afectan a los ciudadanos.		
AUTOR(ES)	Dany Oswaldo Chiluisa Mullo		
REVISOR(ES)/TUTOR(ES)	Dra. Ángela María Paredes Cavedo		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Jurisprudencia, ciencias sociales y políticas		
CARRERA:	Derecho		
TITULO OBTENIDO:	Abogado de los Tribunales y Juzgados de la República del Ecuador.		
FECHA DE PUBLICACIÓN:	23 de febrero de 2021	No. DE PÁGINAS:	26
ÁREAS TEMÁTICAS:	Informática jurídica, derecho penal, ciencia jurídica		
PALABRAS CLAVES/ KEYWORDS:	anomias, delitos informáticos, tutela efectiva, fraude		
RESUMEN/ABSTRACT (150-250 palabras):	El sistema jurídico ecuatoriano contiene un amplio andamiaje normativo a través del cual se garantiza la protección jurídica de las personas. Bajo este contexto, de forma simultánea se presenta también una serie de vacíos y contraposiciones normativas en razón de que los continuos avances jurídicos requieren fortalecer esfuerzos a fin de ir a la par de la evolución social y tecnológica. De modo que, el desarrollo tecnológico trae consigo una nueva corriente delictiva, la cual no se encuentra tipificada en su totalidad debido a la dificultad que implica su regulación al trascender fronteras. Por esta razón, el objetivo de este trabajo de investigación ha sido “elaborar un ensayo crítico jurídico en evidencia de los vacíos legales existentes en el ordenamiento jurídico ecuatoriano y que tienen relación con los delitos informáticos que actualmente afectan a los ciudadanos”. Para el efecto, se cuenta con un sustento bibliográfico, doctrinario y legal preciso, mismo que dentro de un enfoque cualitativo se ha constituido en el principal soporte para la elaboración de este trabajo. Finalmente, luego de exponer la problemática actual que deriva de los vacíos jurídicos expuestos se contrasta la realidad social y normativa para posteriormente plantear posibles soluciones.		
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-3-801364 / +593-987235726	E-mail: dannychiluisa@hotmail.com	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE)::	Nombre: Ab. Toscanini Sequeira Paola María, Msc.		
	Teléfono: +593-999570394		
	E-mail: paola.toscanini@cu.ucsg.edu.ec paolats77@icloud.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			