Fecha de presentación: septiembre, 2020, **Fecha de Aceptación**: noviembre, 2020, **Fecha de publicación**: enero, 2021

48

ANÁLISIS CONCEPTUAL DEL DELITO INFORMÁTICO EN ECUADOR

CONCEPTUAL ANALYSIS OF COMPUTER CRIME IN ECUADOR

Marco Fernando Saltos Salgado[1]
E-mail: us.marcosaltos@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-0445-3571
José Luis Robalino Villafuerte[1]
E-mail: us.joserobalino@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-0478-4338
Lenin Darío Pazmiño Salazar[1]
E-mail: us.leninpazmino@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-0587-9662
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. ***Revista Conrado, 17(78)***, 343-351.

RESUMEN

De acuerdo a diferentes consultas bibliográficas, los delitos informáticos son los de mayor crecimiento en los últimos años en América Latina, con una proyección cada vez mayor, por tal motivo la importancia y pertinencia elevada de su estudio. La investigación pretende ofrecer una herramienta para comprender de mejor forma la problemática del delito informático desde del punto vista conceptual y jurídico. Presenta como objetivo elaborar un mapeo conceptual y análisis jurídico como herramienta para comprender el ciberdelito en Ecuador. Para lograr este fin se emplearon diversos métodos de análisis como el mapa conceptual, análisis histórico y jurídico. Los resultados obtenidos evidencian empíricamente que existen factores como el avance propio de la tecnología de la información que conllevan al aumento de los delitos informáticos, y por tanto es de vital importancia un mejor análisis jurídico de su tipificación.

Palabras clave:

Delito informático, mapa conceptual, análisis jurídico, diagrama de redes.

ABSTRACT

According to different bibliographic consultations, computer crimes are the fastest growing in recent years in Latin America, with a growing projection, for this reason the importance and high relevance of their study. The research aims to offer a tool to better understand the problem of computer crime from a conceptual and legal point of view. Its objective is to develop a conceptual mapping and legal analysis as a tool to understand cybercrime in Ecuador. To achieve this end, various methods of analysis were used, such as the conceptual map, historical and legal analysis. The results obtained empirically show that there are factors such as the advancement of information technology that lead to an increase in computer crimes, and therefore a better legal analysis of their classification is of vital importance.

Keywords:

Computer crime, conceptual map, legal analysis, network diagram.

INTRODUCCIÓN

El vertiginoso desarrollo tecnológico, la interdependencia económica, la desmedida informatización de la sociedad y el omnímodo poder de la Informática, han demandado de la moderna Ciencia Penal, la comprensión de las conductas criminales en las que se ve inmersa la informática (Almenar Pineda, 2017). El incremento de la ciberdelincuencia tiene su fundamentación en varios factores: por una parte, el aumento de tecnología disponible, tanto para el delincuente como las víctimas, y por otra el crecimiento sostenido del mercado negro de la información.

El ciberdelito, al igual que otras figuras penales, ha sido objeto de análisis por parte de juristas y expertos en seguridad informática de todo el mundo; lo que permitió que muchas legislaciones del continente americano tipifiquen conductas ciberdelictuales, tomando en consideración lo que se ha analizado doctrinalmente y tipificado en otros continentes. Según Almenar Pineda (2017), los ciberdelitos o delitos informáticos son vulneraciones que sufren los internautas por parte de delincuentes que roban información personal para usarla en beneficios de ellos.

El modus operandi de los ciberdelincuentes varía de acuerdo con el intelecto y métodos de convencimientos que ellos poseen, medios que van desde correos falsos de entidades bancarias, links de páginas falsas, premios engañosos, virus, entre otros. Los delitos informáticos conllevan engaño, fraude, robo extorsión y otros tipos de delitos asociados.

Las actividades informáticas delictivas están en crecimiento a nivel global, incluyendo a América Latina. En el Ecuador en el año 2009 se empieza a hablar de delitos informáticos registrándose hasta el 2013 un total de 3,143 casos, esto a pesar de que se conoce que el 80% de los delitos informáticos no son reportados, en cuanto al índice delictivo. Ecuador ocupa el tercer lugar después de México con el 92 % y Bolivia con el 85 %, lo que a criterio de la ONU se produce como consecuencia de la falta de una cultura de denuncia. Según una publicación de fecha 30 de enero del 2015 del diario El Comercio (2015), Ecuador ocupa el octavo lugar entre los países de la región que más ataques informáticos registró en el 2014. Brasil y Perú lideran la lista con un 32% y 28% respectivamente.

En el estudio realizado por Temperini (2013), concluyó que los países latinoamericanos presentan una falta de homogeneización en el ámbito sustantivo de la normativa penal aplicable a los delitos informáticos, se destaca la necesidad de mejorar los niveles de armonización y actualización legislativa en la materia, a fin de mitigar la existencia de paraísos legales en la región que favorezcan la ciberdelincuencia. Para el caso de Ecuador este estudió arribó como resultado la posición número 12 en el ranking presentado para los países latinoamericanos, con un 63% de representación de la sanción penal en la legislación vigente del país para los delitos informáticos analizados.

El principal objetivo de estudio es elaborar un análisis jurídico ante la normativa legal de Ecuador sobre los delitos informáticos además de esclarecer su terminología y contenido a través de un mapa conceptual. Los resultados obtenidos permiten analizar información relevante de acuerdo con el tema de estudio, concluyendo que el delito informático ha aumentado en América Latina en la última década, con el avance propio de la tecnología de la información, por tanto, se ha diversificado lo que conlleva a un mejor análisis jurídico de su tipificación.

En la última década ha aumentado el número de investigaciones realizadas en la temática en cuestión. Un ejemplo fue el estudio de Ferruzola Gómez & Cuenca Espinoza (2015), que explica cómo responder ante un delito informático, para lo cual el primer paso es basarse en la Ley Ecuatoriana del COIP de acuerdo al caso de delito informático y denunciarlo para la respectiva investigación. La mayoría de los autores analizados plantean que el ciberdelito es fácil de identificar y prevenir, lo único que la ciudadanía necesita es informarse del tema, como también leer las medidas de prevención que proporcionan las entidades bancarias y páginas gubernamentales (Alcívar Trejo, et al., 2015).

En la actualidad debe ampliarse la tipificación del delito informático. Puesto que es una manera para poder sancionar a aquellas personas que tienen como fin afectar el patrimonio, la honra, y muchas veces hasta la vida de las personas (Zambrano Mendieta, et al., 2016).

La tipificación del delito informático en la Ley Penal responde a elementos tales como el sujeto, medio y objeto. Esta afirmación se muestra en la figura 1.

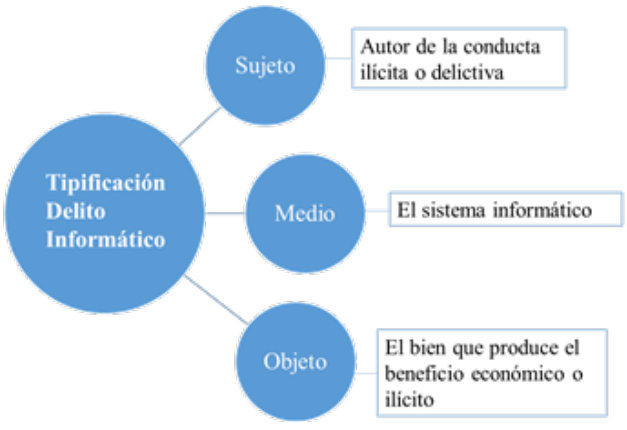

Figura 1. Tipificación del delito.

Tomando en cuenta la tipicidad se identifican dos conceptualizaciones de Delito Informático:

- El concepto típico, corresponde a aquellos delitos informáticos que comprenden conductas típicas, antijurídicas y culpables, mediante las que se hace uso de las computadoras como instrumento o fin.
- El concepto atípico define a los delitos informáticos, como las actitudes ilícitas en donde se usa a las computadoras como medios o fin para delinquir.

El Tratado sobre Delito Informático se le define como un instrumento de carácter internacional que abarca los delitos cometidos mediante el uso del Internet y las redes informáticas, comprende los siguientes delitos:

- Violación por derechos de autor.
- Fraude informático.
- Pornografía infantil.
- Delitos de odio.
- Violaciones de seguridad de red.
- Incautación de datos informáticos.
- Inadecuado uso de dispositivos.
- Delitos relacionados con derechos conexos.
- Interferencia de sistemas.

En la década de los setenta, comienza la extensión del uso de ordenadores en el ámbito empresarial y, con ella, la delincuencia económica relacionada con ellos. En este período estas formas de delincuencia económica son las que predominan a través de la informática e integran lo que se puede identificar como delito informático en un primer momento.

En los años posteriores el uso de los ordenadores se globaliza y no se reduce al ámbito empresarial. Así, en los años ochenta, con el uso extendido de los ordenadores personales, aparecerá la piratería del software y, con ella, las infracciones contra la propiedad intelectual, que se incrementan especialmente en los años noventa, cuando abarcará también música o películas. De esta forma, la aparición internet y su expansión también supone una nueva herramienta de difusión de contenidos ilícitos como la pornografía infantil o la apología del racismo o la xenofobia, o incluso actuaciones contra la seguridad del Estado a través del terrorismo cibernético.

Por último, en el uso de las nuevas tecnologías actualmente concurren una serie de factores, como es un precipitado acceso a ellas, lo que facilita la acción de daños imprudentes en sistemas informáticos, la obstaculización en su normal funcionamiento o incluso el acceso ilícito a ellos. De esta forma, resultan ser numerosos los potenciales ataques a través de la informática, especialmente tras la expansión y uso generalizado de Internet, quedando pocos espacios de la vida que no se vean influidos por procesos de tratamientos de datos, que facilitan también la comisión de delitos tradicionales. Por ello, se puede concluir que hoy en día prácticamente cualquier delito es susceptible de cometerse o verse favorecido a través de estas nuevas herramientas de la información y la comunicación.

En la actualidad no existe una definición en la cual los juristas y estudiosos del derecho estén de acuerdo, es decir un concepto propio de los llamados delitos informáticos. Aun cuando no existe dicha definición con carácter universal, se han formulado conceptos funcionales atendiendo a las realidades concretas de cada país.

Para algunos autores como Guibourg (2015), éste no es más que el delito cometido bajo el empleo de medios informáticos, es decir, constituyen nuevas formas de comisión de conductas ya descritas en sede penal, rechazando la existencia de un bien jurídico autónomo para esta clase de delitos. Para otro sector de la doctrina el delito informático tiene un contenido propio, afectando así un nuevo interés social cuyo reconocimiento legislativo urge, diferenciando así entre delitos computacionales como nuevas formas comisivas de delitos y delitos informáticos, aquellos que afectan el novísimo del bien jurídico penal propuesto.

Finalmente, existe una tercera vertiente, defendida por la doctrina de habla inglesa, que hace una diferencia tripartita en que la informática aparece como medio para cometer delitos tradicionales, como fin en sí misma y como medio de prueba.

La profesora García Cantizano (2012), ha ingresado al debate, considerando que si bien en el Derecho penal no existe un concepto unánime sobre lo que es la delincuencia informática, considera que el delito informático puede definirse, en términos generales, como ***"aquél en el que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos"*** (p. 69-70), con lo que excluye la existencia de un nuevo interés social. Un segundo sector diferencia entre ambas situaciones, esto es, en primer lugar, el uso de la informática como medio novedoso para afectar bienes jurídicos ya resguardados en clave penal, lo que se ha dado por llamar "delito computacional", en tanto que en segundo lugar cataloga aquellas conductas que afectan un nuevo interés social.

Acotando de manera sensata, el profesor Salinas Siccha (2008), nos alcanza una definición acerca del delito

informático, señalando son aquellas conductas típicas, antijurídicas, culpables y punibles, en las que la computadora, sus técnicas y funciones desempeñan un papel trascendente, ya sea como método, medio o fin en el logro de los objetivos indebidos del agente, cual es el logro de algún perjuicio de tipo patrimonial a su víctima. Agrega el citado autor, que también se le podría definir a los delitos informáticos como aquella conducta típica, antijurídica, culpable y punible en la que el agente hace uso de cualquier medio informático para obtener un beneficio indebido en perjuicio del sujeto pasivo.

Existe un tercer sector, minoritario también, postulado por la doctrina norteamericana y británica, que considera que el uso de computadoras se puede manifestar de tres maneras: en la primera, el ordenador puede ser el objeto de la ofensa, en la segunda, la computadora puede ser la herramienta del delito, esto ocurre, según indica los autores que se afilian a esta postura, cuando el sujeto activo utiliza el ordenador para facilitar la comisión de delitos tradicionales, finalmente, en la tercera exteriorización, las computadoras resultan incidentales en los delitos, en la medida que contienen evidencias de los delitos.

Internacionalmente existen diferentes designaciones para la terminología delitos informáticos, tales como, delitos electrónicos, cibercrimen, ciberdelitos, delitos relacionados con las computadoras, crímenes por computadora, entre otros. El término más usado por los autores en la doctrina del derecho penal informático es el de delito informático. Como se señala, es indispensable el uso de la computadora y del manejo del Internet, para la comisión de estas conductas delictivas.

En forma general, las principales características que revisten los Delitos informáticos son:

a. Conductas criminógenas de cuello blanco.
b. Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto se halla trabajando.
c. Son acciones de oportunidad, en cuanto a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d. Provocan serias pérdidas económicas, ya que casi siempre producen “beneficios” de más de cinco cifras a aquellos que los realizan.
e. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g. Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
i. En su mayoría son imprudenciales y no necesariamente se cometen con intención.
j. Ofrecen facilidades para su comisión a los menores de edad.
k. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
l. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Por lo anterior, se puede apreciar que los que cometen este tipo de ilícitos, son personas con conocimientos sobre la informática y cibernética. Que se encuentran en lugares estratégicos o con facilidad para poder acceder a información de carácter delicado, como puede ser a instituciones crediticias o del gobierno. Dañan en la mayoría de los casos el patrimonio de la víctima, la cual, por la falta de una ley aplicable al caso concreto, no es denunciada quedando impune estos tipos de conductas antisociales.

Las conductas o acciones que considera las Naciones Unidas como delitos informáticos son las siguientes:

I. Los Fraudes cometidos mediante manipulación de computadoras: este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común.
II. La manipulación de programas; este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas que tienen conocimiento especializados en programación informática.
III. La Manipulación de datos de salida; se efectúa fijando un objetivo al funcionamiento del sistema informático, el ejemplo más común es el fraude que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.
IV. Fraude efectuado por manipulación informáticas de los procesos de cómputo.
V. Falsificaciones informáticas; cuando se alteran datos de los documentos almacenados en forma computarizada.
VI. Como instrumentos; las computadoras pueden utilizarse también para efectuar falsificación de documentos de uso comercial
VII. Sabotaje Informático; es el acto de borrar, suprimir o modificar sin autorización funciones o datos de

computadora con intención de obstaculizar el funcionamiento normal del sistema.

VIII. Los Virus; Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. -

IX. Los Gusanos; los cuales son análogos al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.

X. La Bomba lógica o cronológica; la cual exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro.

XI. Acceso no autorizado a servicios u sistemas informáticos; esto es por motivos diversos desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

XII. Piratas Informáticos o Hackers; este acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones.

XIII. Reproducción no autorizada de programas informáticos de protección legal; la cual trae una pérdida económica sustancial para los propietarios legítimos.

El Código Penal ecuatoriano ha transitado por diversas etapas donde le han realizado varias modificaciones parciales. Uno de esos cambios fue en materia de Delitos Informáticos, donde se adaptaron las figuras penales clásicas a fin de que sea posible su aplicación en este tipo de violaciones. Un gran avance fue La Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, promulgada en 1999, la que representó un gran avance en la búsqueda de un sistema jurídico que nos asegure confianza a los usuarios de la tecnología. En el 2002 se introdujo a esta ley cambios interesantes en el incompleto panorama de los delitos informáticos.

A nivel internacional en la Convención de Cibercriminalidad de Budapest (Consejo de Europa, 2001), se listan los tipos penales considerados como delitos informáticos: Acceso ilícito (art. 2); Interceptación ilícita (art. 3); Atentados contra la integridad de los datos (art. 4); Atentados contra la integridad del sistema (art. 5); Abuso de equipos (art. 6); Falsedad Informática (art. 7); Estafa Informática (art. 8), e Infracciones relativas a la pornografía infantil (art. 9).

En esta temática en Ecuador, específicamente la Ley No 67 (Ecuador. Congreso Nacional, 2002) regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "De las infracciones informáticas", los artículos del 57 al 64 sancionan los siguientes delitos informáticos: 1) la violación al derecho a la intimidad en documentos con soporte electrónico (Art 58 y 64); 2) la violación o divulgación de información secreta contenida en documentos con soporte electrónico (Art. 58); 3) La obtención y utilización no autorizada de información (Art. 58); 4) la destrucción o supresión de documentos con soporte electrónico por parte de personas que tuvieren su resguardo a cargo (Art. 59); 5) la falsificación electrónica (Art. 60); 6)- los daños informáticos (Art. 61), 7) la apropiación ilícita (Art. 62) y, 8) la estafa utilizando medios electrónicos o telemáticos (Art. 63). Por otra parte, los delitos informáticos también están tipificados en el marco jurídico legal del Ecuador, en el Código Orgánico Integral Penal (COIP) del 2014, como se muestra en la tabla 1 cada artículo con su enunciado y sentencia.

Tabla 1. Tratamiento del Delito informático en el COIP.

Tipicidad del delito informático en el Código Orgánico Penal Integral del Ecuador		
Artículo	Enunciado del delito	Sentencia
190	Apropiación fraudulenta por medios electrónicos	Pena privativa de libertad de uno a tres años.
191	Reprogramación o modificación de información de equipos terminales móviles.	Pena privativa de libertad de uno a tres años.
192	Intercambio, comercialización o compra de información de equipos terminales móviles	Pena privativa de libertad de uno a tres años.
193	Reemplazo de identificación de terminales móviles.	Pena privativa de libertad de uno a tres años.
194	Comercialización ilícita de terminales móviles	Pena privativa de libertad de uno a tres años.
211	Supresión, alteración o suposición de la identidad y estado civil. - La persona que ilegalmente impida altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos	Pena privativa de libertad de uno a tres años.
229	Revelación ilegal de base de datos	Pena privativa de libertad de uno a tres años.
231	Transferencia electrónica de activo patrimonial	Pena privativa de libertad de tres a cinco años.
232	Ataque a la integridad de sistemas informáticos	Pena privativa de libertad de tres a cinco años.
233	Delitos contra la información pública reservada legalmente	Pena privativa de libertad de cinco a siete años.
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	Pena privativa de libertad de tres a cinco años.

298 Inciso 8	Defraudación tributaria: Altere libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.	Pena privativa de libertad de uno a tres años

A modo resumen se plantea, que en el caso del análisis jurídico tanto en el ámbito nacional como internacional para la temática del delito informático ha ocurrido una evolución histórica. Declarada en la perfección de los tratamientos legislativos realizados en el tema en cuestión, como se evidencia en la figura 2.

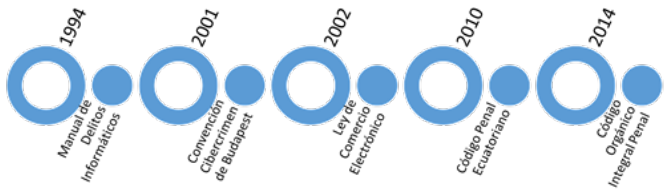

Figura 2. Evolución histórica del tratamiento legal al delito informático.

MATERIALES Y MÉTODOS

Para la realización de esta investigación fue necesario el empleo de métodos tanto teóricos, empíricos como herramientas de análisis de la propia ciencia jurídicas que a continuación se describen:

- Inductivo–deductivo: este método se utilizó en todas las etapas de la investigación, permitió extraer la información necesaria para fundamentar la teoría del delito informático en el proceso jurídico penal y llegar a las conclusiones.
- Analítico–sintético: este método se empleó en la investigación para el análisis y posterior determinación de la correcta concepción del ciberdelito por parte de los sujetos procesales.
- Sistémico: este método se utilizó para conocer de forma detallada todo lo referente al delito informático, permitió el análisis de sus componentes por separado para luego unificar el resultado del proceso como conjunto.
- Método particular de las ciencias jurídicas: la investigación se desarrolló mediante la compilación de autores nacionales y extranjeros, así como todas las normativas legales que sobre el tema se establecen en Ecuador.

Además, se emplearon los siguientes instrumentos:

- Técnica de observación: Esta técnica ayudó a captar los hechos. Objeto o fenómeno para investigar.
- Fichas de observación: para recoger los datos obtenidos en el campo de la investigación.
- Diagrama de redes: para determinar palabras claves principales sobre el concepto analizado.
- Mapa Conceptual: para realizar una representación esquemática sobre el concepto y sus contenidos y relaciones.

Se utilizó el software Ucinet 6.0 para el análisis de red por autores; y CmapTools para la elaboración del mapa conceptual como herramienta ideal para ejercitar la síntesis de los contenidos y estructurar las relaciones existentes entre ellos, la cual se puede encontrar en: https://cmaptools.softonic.com/

RESULTADOS Y DISCUSIÓN

A continuación, se presenta como resultado de la investigación, en un primer lugar, la importancia que reviste para los autores de las ciencias jurídicas penales el análisis del delito informático dentro del derecho penal, en consonancia con el aumento de su ocurrencia en diversas partes del mundo como resultado de los avances tecnológicos alcanzados por la humanidad en cuanto a la informática.

Para ello se realiza un análisis de red que se muestra en la figura 3, como consulta de doce investigaciones de especialistas de esta área de la ciencia comprendido en el período desde el 2013 hasta la fecha, empleando el software estadístico ***UCINET6.0,*** donde se obtuvo como resultado un 78% de densidad de la red. Los autores según refleja la red se asocian en un gran grupo de autores (Temperini, 2013; Alcívar Trejo, et al., 2015; Cano Vargas, 2015; Arroyo Jácome, 2016; Zambrano Mendieta, et al., 2016; Posada Maya, 2017; Quevedo González, 2017; Narváez Montenegro & Recalde Machado, 2018; Ortiz Campos, 2019; López Gorostidi, 2020). Al realizar el análisis, la red muestra una fuerte centralidad en las variables: delito informático y derecho penal, lo que evidencia que la mayoría de los autores le otorgan gran importancia al análisis jurídico penal que debe someterse en el caso de los ciberdelitos.

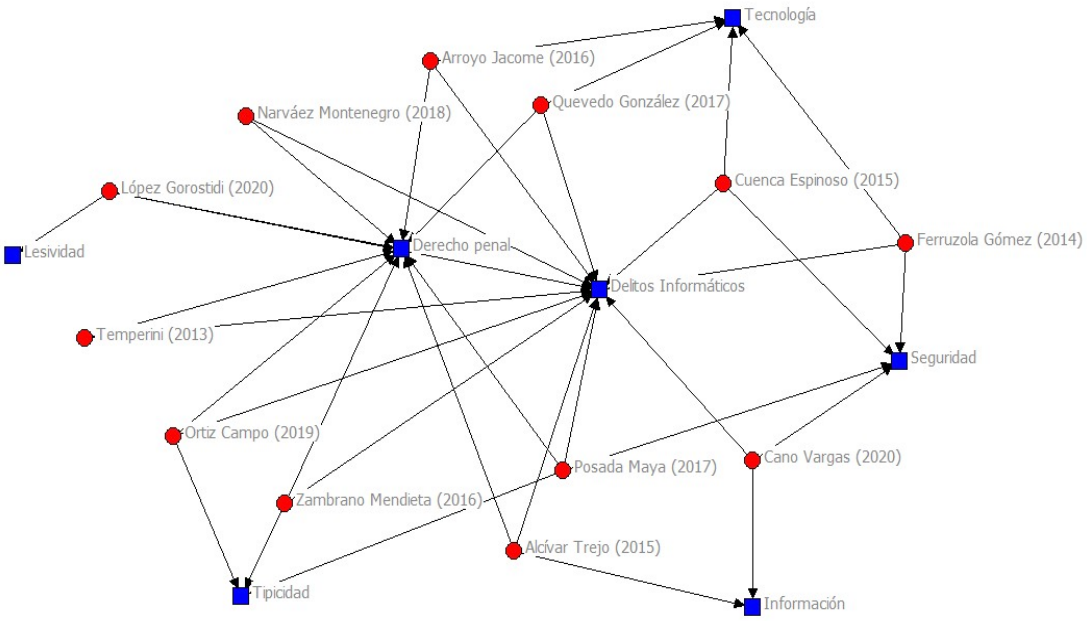

Figura 3. Análisis de red del delito informático por autores.

Por otra arista del análisis se decide realizar un mapa conceptual al concepto de delito informático que permite su mejor comprensión al desagregarlo en cada componente que lo compone. Puesto que la principal forma de analizar la representación de conceptos son los mapas conceptuales pues son la única técnica que se basa en las teorías del aprendizaje significativo y del conocimiento de ahí su importancia como técnica para la comprensión (Jorna Calixto & Véliz Martínez, 2019).

A través de los años se han manejado diferentes definiciones de mapas conceptuales, pero la más arraigada es la presentada por Novak en el año 1988 (Simón Cuevas, 2003) como técnica que representa, simultáneamente, una estrategia de aprendizaje, un método para captar lo más significativo de un tema y un recurso esquemático para representar un conjunto de significados conceptuales, incluidos en una estructura de proposiciones. Como su nombre lo indica, es una representación gráfica formada por elementos conceptuales (nodos o centros) que forman redes, unidos por relaciones que pueden ser asociativas, causales o temporales que dan sentido a la representación de las categorías.

El uso de los mapas conceptuales pronto se ha extendido por todo el mundo como una forma de representar el conocimiento de una persona sobre un tema, siendo realizados por usuarios de todas las edades y en todos los dominios del conocimiento. Una de las tantas aplicaciones de mapas conceptuales es organizar y representar las ideas principales de un tema de estudio de una manera breve y simple (García Tormo, 2020; Urrejola Contreras, et al., 2020).

Se propone su aplicación para comprender el delito informático en su análisis dentro del derecho jurídico penal. La necesidad de aplicar la herramienta a este ámbito está dada por su compatibilidad con la complejidad y la relación subjetividad-objetividad inherente al tema, tomando como base las ventajas expuestas con anterioridad. Luego del análisis de red realizado, se construye el mapeo conceptual diseñado para la comprensión del delito informático como se refleja en la figura 4.

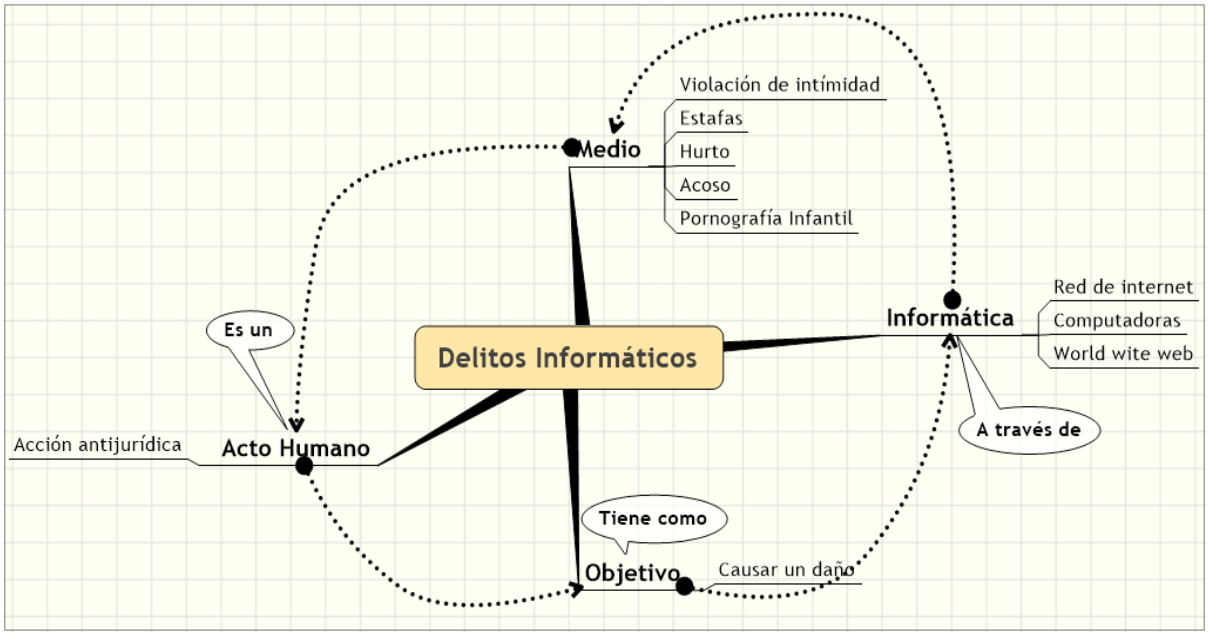

Figura 4. Mapa conceptual del delito informático.

En el análisis del mapa conceptual propuesto se refleja que un delito informático es una violación jurídica humano que provoque lesión o daño, mediante el empleo de la computadora. Su concepción a través del mapa conceptual permite un mejor análisis al desintegrar el concepto en sus dimensiones y aspectos principales.

CONCLUSIONES

La ley en el Ecuador es generalizada en el tema de delitos informáticos, por lo cual, necesita ser reformada y especificada acorde a cada tipo de delito y estar en constante actualización mediante los cambios en la sociedad y la tecnología para proporcionar seguridad a los internautas.

Tomando como referencia los conceptos dados por diversos autores se ha logrado establecer que existen factores como el avance propio de la tecnología de la información que conllevan al aumento de los delitos informáticos, y por tanto es de vital importancia un mejor análisis jurídico de su tipificación.

El mapa conceptual permite comprender el delito informático desde su concepción, lo que pudo establecer con claridad los elementos que lo integran, objetivo que persigue, medios que se emplean, entre otros aspectos.

REFERENCIAS BIBLIOGRÁFICAS

Alcívar Trejo, C., Doménech Alvarez, G. A., & Ortiz Chimbo, K. M. (2015). La seguridad jurídica frente a los delitos informáticos. AVANCES, 10(12), 41-41.

Almenar Pineda, F. (2017). El delito de hacking. Universitat de València.

Arroyo Jácome, R. P. (2016). Análisis de los delitos informáticos por ataque y acceso no autorizado a sistemas electrónicos, tipificados en los artículos 232 y 234 del Código Orgánico Integral Penal en el Ecuador. (Proyecto de Investigación). Universidad Central del Ecuador.

Cano Vargas, J. (2015). Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA. (Trabajo de grado). Universidad Nacional Abierta y a Distancia.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Diario El Comercio, D. (2015). Cómo evitar los ataques de las cibermafias. https://www.elcomercio.com/app_public.php/actualidad/evitar-ataques-cibermafias.html

Ecuador. Congreso Nacional. (2002). Ley No 67. Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos. Registro Oficial N. 557. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Ferruzola Gómez, E. C., & Cuenca Espinoza, H. A. (2015). Cómo responder a un Delito Informático. *Ciencia Unemi*, *7*(11), 43-50.

García Cantizano, M. d. C. (2012). Delincuencia informática en el ordenamiento jurídico penal peruano. Gaceta Jurídica–N78B, 69-72.

García Tormo, J. V. (2020). Mapas conceptuales como instrumento de coordinación docente en estudios de posgrado. Revista INFAD de Psicología. International Journal of Developmental and Educational Psychology., 2(1), 257-264.

Guibourg, R. A. (2015). Informática jurídica. Información Jurídica, 1, 791-823.

Jorna Calixto, A. R., & Véliz Martínez, P. L. (2019). Mapa conceptual como herramienta de aprendizaje gerencial de los procesos de promoción en Cuba. Revista Cubana de Salud Pública, 45(4).

López Gorostidi, J. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. Estudios de Deusto: revista de la Universidad de Deusto, 68(1), 201-221.

Narváez Montenegro, B. D., & Recalde Machado, G. E. (2018). El delito informático en América. Debate Jurídico Ecuador, 1(1), 3-14.

Ortiz Campos, N. J. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos 21, 4(1), 100-111.

Posada Maya, R. (2017). Los cibercrímenes: Un nuevo paradigma de criminalidad.: Un estudio del título VII bis del Código Penal colombiano. Ediciones Uniandes-Universidad de los Andes.

Quevedo González, J. (2017). Investigación y prueba del ciberdelito. Universitat de Barcelona.

Salinas Siccha, R. (2008). Derecho penal. Parte especial, 5.

Simón Cuevas, A. J. (2003). Propuesta de aplicación de los mapas conceptuales en un modelo pedagógico semipresencial. *Revista Iberoamericana de Educación*, *33*(2), 1-11.

Temperini, M. G. I. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. http://elderechoinformatico.com/publicaciones/mtemperini/CONAIISI_Temperini_Camera_Ready.pdf

Urrejola Contreras, G. P., Lisperguer Soto, S., Calvo, M. S., Pérez Lizama, M. A., Tenore Venegas, P., & Pérez Casanova, D. (2020). Uso de mapas conceptuales en Razonamiento Clínico como herramienta para favorecer el rendimiento académico. Educación Médica Superior, 34(1).

Zambrano Mendieta, J. E., Dueñas Zambrano, K. I., & Macías Ordoñez, L. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. Dominio de las ciencias, 2(2), 204-215.