Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VIII. Vol. VIII. N° 1. Edición Especial. 2023
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

https://doi.org/10.35381/racji.v8i1.3339

Los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano

Computer crimes in the Ecuadorian Organic Integral Criminal Code

Seidy Gabriela Tixi-Janeta
pg.seidygtj19@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0009-0009-3698-3997

María Lorena Merizalde-Avilés
ua.mariamerizalde@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0001-5289-8949

Ariel José Romero-Fernández
ua.arielromero@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-1464-2587

Genaro Vinicio Jordán-Naranjo
ua.genarojordan@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-3027-3926

Recibido: 15 de mayo 2023
Revisado: 20 junio 2023
Aprobado: 15 de agosto 2023
Publicado: 01 de septiembre 2023

Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas
Año VIII. Vol. VIII. N° 1. Edición Especial. 2023
Hecho el depósito de Ley: FA2016000064
ISSN: 2542-3371
FUNDACIÓN KOINONIA (F.K). Santa Ana de Coro, Venezuela

RESUMEN

El objetivo general de la investigación fue analizar jurídicamente los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano. La presente investigación utilizó el método cuantitativo, se apoyó en la revisión documental-bibliográfica. Además, se aplicó el método inductivo-deductivo. Se planteó además el método analítico-sintético. Se puede concluir que, el COIP cubre de forma media el juzgamiento de los delitos informáticos, se deben incluir el cyberbullying, ciberterrorismo, liderar bandas criminales para delitos informáticos y secuestro cibernético. Sobre las penas se mencionan cambios como aumento y disminución de pena para delitos específicos. Adicionalmente, se tiene un consenso a que no existe ambigüedad o una incorrecta redacción de los artículos del COIP.

Descriptores: Delito informático; legislación; derecho penal. (Tesauro UNESCO).

ABSTRACT

The general objective of the research was to legally analyze computer crimes in the Ecuadorian Organic Integral Criminal Code. The present research used the quantitative method, based on the documentary-bibliographic review. In addition, the inductive-deductive method was applied. The analytical-synthetic method was also used. It can be concluded that the COIP covers in an average way the prosecution of computer crimes, cyberbullying, cyberterrorism, leading criminal gangs for computer crimes and cyber kidnapping should be included. Regarding penalties, changes such as increased and decreased penalties for specific crimes are mentioned. Additionally, there is a consensus that there is no ambiguity or incorrect wording of the articles of the COIP.

Descriptors: Computer crime; legislation; criminal law. (UNESCO Thesaurus).

INTRODUCCIÓN

El desarrollo de la tecnología informática, ha permitido la mejora y optimización de los procesos organizacionales y se ha convertido en una herramienta imprescindible de almacenamiento y gestión de información para empresas e instituciones. La pandemia mundial del COVID-19 ha marcado un punto de inflexión fundamental en nuestra senda mundial y ha acentuado como nunca antes nuestra dependencia de la infraestructura digital (BID y OEA, 2020). Sin embargo, así como ha permitido un avance notable al ser humano, también ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables.

Al delito informático se lo puede definir como cualquier actividad en la cual, a través del uso de las computadoras, se comete un delito, estos pueden constituirse en nuevas formas penales donde se incluyen como elementos primarios al internet y a la computadora como instrumentos físicos (Wang, 2016,). Según Almenar (2017) los delitos informáticos son vulneraciones que sufren los internautas por parte de delincuentes que roban información personal para usarla en beneficios de ellos. Por lo tanto, el delito informático se define como una actividad delictiva en la cual intervienen medios informáticos o electrónicos.

Los regímenes legales están desarrollando diversas estrategias destinadas a reducir el riesgo que representan las infracciones cibernéticas, y la legislación es una parte indispensable de su estrategia. Sin embargo, la investigación ha identificado la efectividad limitada de las legislaciones para abordar los delitos informáticos (Wang, 2016). En el Ecuador en el último año se han incrementado una serie de delitos informáticos, solo hasta el mes de mayo de 2021 existieron más de 600 denuncias por esta causa, así lo menciona el diario El Universo en su publicación del 25 de mayo de 2021. Según cifras oficiales de la Policía Nacional del Ecuador, hasta agosto de 2021 se abrieron más 1200 investigaciones por delitos informáticos en el Ecuador. La dificultad surge al tratar de aplicar las normas existentes nuevos delitos informáticos, con características específicas por esta razón se genera la necesidad de que el gobierno regule y sancione todo tipo de actividades donde se utiliza la informática con ánimo doloso o culposo.

En la presente investigación se plantea como objetivo general analizar jurídicamente los delitos informáticos en el Código Orgánico Integral Penal ecuatoriano.

MÉTODO

La presente investigación utiliza el método cuantitativo, apoyado en la revisión documental-bibliográfica. Además, se aplica el método inductivo-deductivo, el cual sugiere que para encontrar una verdad se deben buscar los hechos y no basarse en meras especulaciones, además de partir de afirmaciones generales para llegar a específicas (Dávila, 2006). Se plantea además el método analítico-sintético por medio del cual, se descompone un todo en partes extrayendo cualidades, componentes, relaciones y más para posteriormente unir las partes analizadas y con ello descubrir características y relaciones entre los elementos (Rodríguez y Pérez, 2017).

RESULTADOS

En el mundo 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 ciber delictuales, tomando en consideración lo que se ha analizado doctrinalmente y tipificado en otros continentes, un sistema de clasificación interesante es el definido por el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Se distinguen cuatro infracciones: (1) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, (2) delitos informáticos, (3) delitos relacionados con el contenido y (4) delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Gercke, 2009).

El departamento de justicia de los Estados Unidos divide al delito informático (cybercrime) en tres categorías, (1) delitos en los que la computadora o la red informática es el objetivo de una actividad delictiva, como piratería y deterioro de un sistema informático; (2) delitos tradicionales en los que la computadora es una herramienta utilizada para cometer el delito, como la pornografía infantil y el fraude en línea; y (3) delitos en los que el uso de la computadora es un aspecto incidental de la

comisión del delito, pero puede proporcionar evidencia del delito, como direcciones encontradas en la computadora de un sospechoso de asesinato. De forma similar lo realiza Australia con la diferencia de que en Estados Unidos el vandalismo y la invasión del espacio personal pertenecen a delitos convencionales, mientras que en la clasificación australiana están en el grupo de piratería y deterioro de los sistemas informáticos (Wang, 2016).

Según Rojas (2016), el cual hace un estudio de la penalización del cibercrimen (o delito informático) en países de habla hispana, Republica Dominicana lidera en la cantidad de delitos tipificados, seguido de Paraguay, Costa Rica, México y Venezuela; Ecuador se encuentra en la posición seis de esta lista. Los países con menor cantidad de delitos tipificados hasta la fecha de publicación del artículo en mención son Honduras, Bolivia y Uruguay. Se indica, además, que las penas máximas para delitos informáticos lo lideran Republica dominicana con 30 años seguido de Costa Rica, Colombia, Ecuador y Honduras. Y con penas mínimas se encuentran los países de Paraguay, El Salvador y Puerto Rico. Uruguay y Bolivia son los países donde los delitos informáticos no implican la privación de la libertad.

Se muestra la clasificación del delito informático según Gercke (2009), en su documento El Ciberdelito: Guía para los Países en Desarrollo patrocinado por la Unión Internacional de Telecomunicaciones presenta una clasificación que se considera completa con respecto a los delitos informáticos, esta ha sido utilizada como base para esta investigación:

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

A.1. Acceso ilícito (piratería de sistemas y programas): Entre estos se tiene la irrupción en sitios web protegidos con contraseña, la burla de la protección de contraseña en un computador, la utilización de equipos o programas para obtener una contraseña e irrumpir en el sistema informático, la creación de sitios web "falsos" para lograr que el usuario revele su contraseña, la instalación por hardware y software de interceptores de teclado ("keyloggers").

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

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

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

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

Delitos relacionados con el contenido.

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

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

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

B.4. Delitos contra la religión, en algunos países se presentan normas jurídicas relacionadas a la religión y es un delito atentar contra la misma, como realizar declaraciones antirreligiosas, crear contenido que genere polémica o burla a los aspectos y creencias religiosas.

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

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

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

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

Delitos en materia de derechos de autor y de marcas

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

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

Delitos informáticos

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

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

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

D. 4. Utilización indebida de dispositivos, Pueden encontrarse herramientas que simplifican el cometer delitos informáticos como el correo basura, las descargas de archivos, que se utilizan para cometer ataques por denegación de servicio, diseñar virus informáticos, desencriptar información o acceder en forma ilegal a sistemas informáticos.

DISCUSIÓN

Según Saltos (2015), el artículo 185 del COIP, es un delito informático, a pesar de que no mencione que este puede realizarse por un medio electrónico o digital, se entiende que el delito de extorsión será juzgado por igual, si la persona incurre a este acto por cualquier medio. En contraste el artículo 186, “estafa” de esta misma ley, si menciona en sus numerales una relación de pena máxima de una defraudación con el uso de tarjetas de crédito, débito o similares (numeral 1) y con el uso de dispositivos electrónicos (numeral 2). Cuando se produce un delito de estafa también puede incurrir a cometer el delito de suplantación de identidad (artículo 212), tal es el caso de que extraiga información confidencial bancaria de una persona con una simulación de hechos falsos, ofreciendo uno u otro servicio y posteriormente suplante a la misma con la finalidad de obtener un beneficio que generalmente es económico.

Según Bolaños y Gómez (2015), los artículos del COIP que juzgan el delito informático son: El artículo 103 (Pornografía con utilización de niñas, niños o adolescentes), el artículo 178 (violación a la intimidad). Además, se encuentran los artículos 180, 182, 195, 230, en los cuales existe una clara relación con delitos informáticos. Los artículos 453, 454, 472, 475, 476, 477, 498, 499, 500 y 511, pertenecen a conceptos,

procedimientos legales de aplicación de esta ley, que guardan relación al ámbito informático.

CONCLUSIONES

Se puede concluir que el COIP cubre de forma media el juzgamiento de los delitos informáticos, se deben incluir el cyberbullying, ciberterrorismo, liderar bandas criminales para delitos informáticos y secuestro cibernético. Sobre las penas se mencionan cambios como aumento y disminución de pena para delitos específicos. Adicionalmente, se tiene un consenso a que no existe ambigüedad o una incorrecta redacción de los artículos del COIP y solo se exponen algunos criterios de mejora. También, se cree que el juzgamiento de este delito depende en gran medida de los operadores de justicia y el conocimiento de la sociedad de los delitos informáticos.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes, por motivar el desarrollo de la Investigación.

REFERENCIAS CONSULTADAS

Almenar, F. (2017). El delito de hacking. [The crime of hacking]. Tesis Doctoral. Universitat de Valencia. https://n9.cl/e0hxi

Asamblea Nacional. (2014). Código Orgánico Integral Penal. [Comprehensive Criminal Code]. Registro Oficial Nº 180. https://url2.cl/53c6h

Banco Interamericano de Desarrollo., y Organización de los Estados Americanos. (2020). Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. [Cybersecurity 2020 Report: Risks, Progress and the Way Forward in Latin America and the Caribbean]. https://doi.org/10.18235/0002513

Bolaños Burgos, F., y Gómez Giacoman, C. (2015). Estudio cualitativo de la relación de las leyes y la pericia informática en el Ecuador. [Qualitative study of the relationship between laws and computer expertise in Ecuador]. *ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica*, (3). https://n9.cl/65qqew

Dávila Newman, G. (2006). El razonamiento inductivo y deductivo dentro del proceso investigativo en ciencias experimentales y sociales. [Inductive and deductive reasoning within the research process in experimental and social sciences*]. Laurus*, *12*(Ext), 180-205. https://n9.cl/nx847

El Universo. (2021, mayo 25). Más de 600 denuncias por delitos cibernéticos se han registrado en Ecuador en lo que va del 2021. [More than 600 cybercrime complaints have been registered in Ecuador so far in 2021]. https://n9.cl/tt1ed

Gercke, M. (2009). El ciberdelito: Guía para los países en desarrollo. [Cybercrime: A Guide for Developing Countries].

Rodríguez, A., y Pérez, A. O. (2017). Métodos científicos de indagación y de construcción del conocimiento. [Scientific methods of inquiry and knowledge construction]. *Revista EAN*, *82*, 179-200. https://doi.org/10.21158/01208160.n82.2017.1647

Rojas, J. (2016). Análisis de la penalización del cibercrimen en países de habla hispana. [Analysis of the criminalization of cybercrime in Spanish-speaking countries]. *Logos, Ciencia y Tecnología*, *8*(1). https://doi.org/10.22335/rlct.v8i1.339

Saltos, M., Robalino, J. L., y Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. [Conceptual analysis of computer crime in Ecuador]. *Revista Conrado,17*(78), 343-351. https://n9.cl/nshbh

Wang, Q. (2016). A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. https://n9.cl/6itlj