LA SEXTORSIÓN COMO CIBERDELITO Y LA NECESIDAD DE TIPIFICARLOS EN EL CÓDIGO PENAL HONDUREÑO

SEXTORTION AS A CYBERCRIME AND THE NEED TO CRIMINALIZE IT IN THE HONDURAN PENAL CODE

Aldair Orlando Amador Figueroa[1]

DOI: https://doi.org/10.5377/lrd.v42i1.12928

RESUMEN:

La siguiente investigación tiene como objetivo identificar y demostrar que el Estado de Honduras carece de una normatividad basada en proteger a sus habitantes en materia de ciberseguridad, justificando el estudio al desarrollo continuo de las nuevas tecnologías de información y comunicación que junto con las leyes, deben encaminarse a la construcción de un cuerpo normativo que no de lugar a ningún tipo de delincuencia. Aunado a esto, se incluyen algunas posibles soluciones que puedan dirigir al Estado a cumplir con la seguridad cibernética de la población.

PALABRAS CLAVE: Ciberdelito, Ciberseguridad, Sextorsión, Suplantación de Identidad, Redes Sociales.

ABSTRACT:

The following research aims to identify and demonstrate that the State of Honduras lacks a regulation based on protecting its inhabitants in the area of cybersecurity, justifying the study to the continuous development of the new information and communication technologies that, together with the laws, must be directed to the construction of a normative body that does not give rise to any type of crime. In addition, there are some possible solutions that could lead the State to comply with the cybersecurity of the population.

KEYWORDS: Cybercrime, Cybersecurity, Impersonation, Sextortion, Social Networks.

Fecha de recepción: 28/4/2021
Fecha de aprobación: 01/11/2021

1 Abogado infieri de la Facultad de Ciencias Jurídicas, Universidad Nacional Autónoma de Honduras, correo electrónico: aldair.o.figueroa@gmail.com

I. INTRODUCCIÓN

Las conductas delictivas al igual que el avance de las tecnologías evolucionan y se transforman adaptándose a las condiciones vigentes en el tiempo, es así que los delitos cibernéticos en el siglo XXI representan nuevas formas de delincuencia figurando un desafío nuevo para las ciencias jurídicas. El mundo cada vez está más globalizado en la tecnología, dando paso a nuevas formas de interacción entre las personas lo cual es un arma de doble filo ya que las facilidades que nos provee la tecnología nos hacen susceptibles a ataques en razón de nuestra privacidad.

Las redes sociales son sitios web que ofrecen servicios y funcionalidades de comunicación diversos para mantener en contacto a los usuarios de la red (RUGAMA. & ESPINOZA ALGABA, 2015) que en un principio fueron creadas como un medio por el cual se pretendía establecer conexiones entre las personas comunes en un grupo determinado, esta finalidad se vio tergiversada cuando los grupos delictivos vieron como una oportunidad viable y segura de cometer actos ilícitos sin el riesgo que fueran descubiertos y consecuentemente capturados y judicializados.

Por esta razón, los Estados de diferentes partes del mundo se han visto en la tarea de incluir legislación en materia de ciberseguridad en sus ordenamientos jurídicos, además de fortalecer la cooperación internacional entre estados a través de convenios internacionales como el Convenio de Budapest que es la normativa marco en materia de ciberseguridad como también el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio, que proveen herramientas y disposiciones generales para la prevención, la armonización de las leyes nacionales con las internacionales relativas a la ciberseguridad y la mejora de las técnicas de investigación.

El presente estudio pretende evidenciar la deficiencia en materia de ciberseguridad que presenta el Estado de Honduras y la importancia que tiene el fortalecimiento del ordenamiento jurídico en materia cibernética, comenzando por robustecer la cooperación internacional mediante la suscripción de tratados y convenios internacionales en la materia, la creación de una legislación especializada e independiente que contenga todas las conductas ciber delincuenciales en un solo marco normativo incluyendo la conducta de la sextorsion o extorsión sexual ya que no puede ser calificada como un delito de chantaje o una extorsión porque no reúne las condiciones de los tipos penales de esos delitos.

Del mismo modo, hacer énfasis que mediante la creación de ésta ley especial, que junto con la suscripción a la normativa internacional se logren tutelar los bienes jurídicos violentados por éstas conductas, como ser, los enmarcados en los artículos 61 y 65 de la Constitución de la República, que realzan la inviolabilidad al derecho de la vida y el artículo 76 constitucional que reúne el derecho al honor, a la intimidad y a la propia imagen, esto en razón a la obligación de tutelar estos principios constitucionales, los cuales son ignorados por el Estado.

II. METODOLOGÍA

El presente trabajo es una investigación de tipo aplicada porque en razón del tema de estudio se busca ampliar el marco jurídico hondureño en materia penal y en específico de la ciberseguridad, presenta un diseño no experimental, bajo un enfoque cualitativo porque pretende describir las conductas delictivas en el ámbito de las redes sociales y los efectos de que no estén tipificados en el ordenamiento jurídico de nuestro país como también fortalecer la normativa ya tipificada, utilizando un alcance explicativo ya que se

pretende conocer las razones por las cuales la legislación hondureña no regula en su totalidad los ciberdelitos y las razones del porqué no está adherido a convenios internacionales para regular estas conductas delictivas; empleando fuentes documentales como ser, artículos científicos, doctrinas y legislación de Nicaragua, Costa Rica y República Dominicana haciendo uso del derecho comparado en relación a la legislacion de estos paises, con el objetivo de fortalecer las políticas en materia de ciberseguridad. Por último, se utilizó el método inductivo partiendo de una premisa específica como ser la conducta de la sextorsión hasta concluir con su tipificación en el ordenamiento jurídico hondureño.

III. RESULTADOS

3.1. Sextorsión como conducta delictiva

Para dar inicio al estudio de la conducta de la sextorsion en jóvenes hondureños puede ser consecuencia de la suplantación o robo de identidad en redes sociales y la falta de su tipificación legal en el ordenamiento jurídico partiremos de la revisión bibliografica referente al tema, resulta: La sextorsión según Rugama & Espinoza Algaba (2015) son imágenes íntimas que el delincuente amenaza con hacer llegar a inoportunas manos, poner en circulación a través de terminales móviles o subir a la red. Por otro lado el "Robo de identidad" se define como la apropiación de la identidad de una persona, hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona de acuerdo a Rinaldi (2017).

Siendo la sextorsión un fenómeno reciente, ya que nace con el uso de las tecnologías de comunicación como ser las redes sociales (Sueiras, s.f.) que junto con la suplantación de identidad constituye una nueva forma delictiva que amenaza a la ciberseguridad de los usuarios, es por ello que los Estados son los responsables de adoptar mecanismos, legislaciones para la tutela efectiva de la seguridad juridíca de las personas.

En el caso de Honduras y de Nicaragua se encontró una similitud en el ordenamiento jurídico penal referente a la no regulacion de la figura de la sextorsion como tal, ya que lo regulan de una forma diferente que se reserva a la interpretación del legislador, subsumiéndola en un tipo de chantaje. El Código Penal Hondureño en el Título VIII, Capítulo II, Artículo 247 hace referencia que el chantaje es quien exige a otra persona dinero, bienes, recompensa o la realización u omisión de un acto, bajo la amenaza de revelar, difundir o imputar hechos referentes a su vida privada que pueden afectar a su honor, crédito o prestigio; asimismo, en el artículo 185 del Código Penal de Nicaragua establece la figura del chantaje como el que, con amenaza de imputaciones contra el honor o el prestigio, violación o divulgación de secretos, con perjuicio en uno u otro caso para el ofendido, su familia o la entidad que represente en que tenga interés, obligue a otro a hacer o no hacer algo.

Al hacer el analisis comparativo entre ambos cuerpos normativos se encontro que la sextorsion tiene su origen en el chantaje, ya que el sujeto activo según (RUGAMA. & ESPINOZA ALGABA, 2015) a partir de la posesión por parte del chantajista de una imagen íntima tiene la finalidad de la obtención de dinero, el dominio de la voluntad de la víctima o la victimización sexual de la misma.

Otros autores lo vinculan con la extorsion por su denominacion fonetica "sextorsion" al respecto Rugama & Espinoza Algaba (2015) dice: no tiene

que ver necesariamente con la extorsión, que en castellano se suele usar únicamente para chantajes de carácter económico, pero al calcarse del inglés ha permanecido el término sextorsión, por su fácil fusión con sex; la extorsion según el Código Penal hondureño es regulada en el titulo XX, Delitos contra el patrimonio en el capítulo Vll, artículo 373 que cataloga la figura de la extorsión: quien con violencia o intimidación y ánimo de lucro, obliga o trata de obligar a otro a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero

Al hacer la respectiva comparación de los términos a los cuales le da origen a la conducta de la sextorsión, se encontró que, si bien es cierto, deriva de un chantaje y también puede constituirse como una extorsión, sin embargo, no termina de reunir las condiciones del tipo penal, ya que en el caso del chantaje regulado en el artículo 247 del Código Penal hondureño, exige en su configuración objetiva del tipo penal, que el sujeto activo exija a cambio de la no difusión o imputación de hechos referentes a su vida privada que pueden afectar a su honor, crédito o prestigio, dinero, bienes, recompensa, o la realización u omisión de un acto; sin embargo, este artículo queda a la interpretación del legislador, por lo cual no es claro, ya que la denominación de vida privada según la RAE, se divide en privacidad e intimidad, conceptos que son mutuamente excluyentes porque no constituyen lo mismo; siendo la privacidad el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión y la intimidad es la zona espiritual íntima y reservada de una persona que tiene un carácter más restringido.

Es por ello que en razón a este elemento de la vida privada, no puede calificarse a la sextorsión como un chantaje en su totalidad, además de faltar en la configuración del tipo penal del chantaje un elemento de suma importancia en la conducta de la sextorsión, que es el hecho de ser cometido a través de las tecnologías de la información y la comunicación; del mismo modo, no puede calificarse como una extorsión porque así como lo señala Guevara, Yáñez (2019) falta el elemento normativo del tipo objetivo, esto es la vulneración al derecho a la propiedad, ya que la exigencia del agente delictuoso no es el "animus apropiandi" de bien ajeno, sino más bien tener acceso a más imágenes pornográficas, videos eróticos o actos que afecten la integridad sexual bajo amenaza de publicación de imágenes íntimas de la víctima.

3.2. Región centroamericana y los retos en materia de ciberseguridad y ciberdelincuencia

Según los autores Zambrano & Hernández (2020) del reciente estudio realizado por Ipandetec, la ciberdelincuencia y la ciberseguridad constituyen dos temáticas importantes a analizar en el entorno digital de cada país. La ciberdelincuencia, nace como resultado de los avances tecnológicos. Este método de delinquir se define como aquellos atentados a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de redes y los datos, así como el uso fraudulento de tales sistemas, redes y datos; por otro lado, la ciberseguridad es definida por la Unión Internacional de Telecomunicaciones como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno.

En razon a esto, se dispondrá a comparar la situacion de ciberseguridad y ciberdelincuencia en

los países de Nicaragua, Costa Rica y República Dominicana, relacionando con las regulaciones dispuestas para las materias de ciberseguridad y ciberdelincuencia en Honduras.

Costa Rica en materia de ciberseguridad, según el Informe Global de Ciberseguridad, califica al país como el #18 en América y el #115 global en compromiso en materia de ciberseguridad, además de ser uno de los únicos países de la región de Centroamérica en ratificar el Convenio de Budapest que es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. (Europa, 2001), y que actualmente, cuenta con 63 países miembros. Costa Rica posee, desde el año 2012 un centro de respuestas a incidentes de seguridad informática, equipo que es constituido por expertos en la materia de ciberseguridad, esto con el objetivo de prevenir y responder a ataques y peligros cibernéticos que afectan a las instituciones gubernamentales. Este equipo de respuesta tiene su origen al llamado incidente "gusano Morris" de 2 de noviembre de 1988 en Estados Unidos, que tenía como objeto averiguar las contraseñas de otras computadoras a través de este virus.

Desde el año 2017, Costa Rica cuenta con una estrategia nacional de ciberseguridad, dicho documento marcó la pauta a seguir en materia de ciberseguridad en el país, dando a conocer los retos que se deben de vencer y las áreas a conocer. Si bien es cierto, el Estado de Costa Rica es parte de los adheridos al Convenio de Budapest, pero es importante aclarar que no está suscrito al Llamamiento de Paris para la Confianza y la Seguridad en el Ciberespacio del 12 de noviembre de 2018, el cual consiste en proponer una visión para regular el mundo cibernético y los grandes principios relacionados. Es la primera gran iniciativa internacional que se plantea desde una lógica de inclusión de múltiples actores (Estados, empresas privadas, organizaciones de la sociedad civil).

Los delitos cibernéticos en Costa Rica, están tipificados en la Ley no. 9048 que reforma el título VI del Código Penal. Esta ley busca mejorar la lucha contra la ciberdelincuencia y protege actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como datos personales, la identidad y los derechos de los niños y niñas.

El parlamento costarricense mantiene en su agenda legislativa un proyecto de ley No. 21187 para combatir la Ciberdelincuencia, la iniciativa busca adecuar el marco penal a las exigencias del Convenio de Budapest. Algunos de los delitos tipificados en esta reforma son: el acoso cibernético, captación de actos o partes íntimas, ciberacoso sexual, entre otros.

Costa Rica cuenta con una sección especializada de investigación informática, adscrita al Departamento de Investigaciones Criminales de Ministerio Público, donde se pueden interponer la denuncia de este tipo. Además de esto, establece una cooperación con los proveedores de servicios electrónicos en el marco de una investigación de delitos informáticos y remoción de contenido en casos de acoso cibernético o pornografía infantil dentro de las primeras 24 horas posteriores a la denuncia.

En República Dominicana, al igual que en Costa Rica, se cuenta con un equipo de respuesta a ataques cibernéticos creada en el año 2018, llamada Centro Nacional de Ciberseguridad y

que en conjunto con el Equipo de Coordinación de Estrategias de Ciberseguridad (ECEC) y el Equipo de Respuestas a Incidentes Cibernéticos de la República Dominicana se da respuesta a las emergencias cibernéticas.

Asimismo cuenta con una estrategia de ciberseguridad, establecida en el año 2018 promulgada mediante decreto 230-18 concebida como un conjunto de políticas y acciones que promueven la inclusión de las tecnologías de la información y de las comunicaciones en determinados procesos que tienen como eje la ciberseguridad para el desarrollo de un Estado digital. De igual forma, la constitución política reconoce como derecho fundamental la intimidad y el respeto al honor personal.

República Dominicana es un país pionero en cuanto a legislación porque posee con diversos mecanismos de regulación en materia cibernética como ser la Ley no. 53-07 sobre Crímenes y Delitos de Alta Tecnología que contiene apartados importantes en consonancia con el Convenio de Budapest como ser las disposiciones específicas de la obtención en tiempo real de datos sobre el tráfico y sobre el contenido.

El país es parte del Convenio de Budapest, siendo el primero en formar parte en la región. Por otro lado, también forma parte del Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio; República Dominicana es uno de los pocos países firmantes en América Latina. República Dominicana cuenta con tribunales y agencias de investigacion especializadas en materia de cibercriminalidad, como ser: el Departamento de Investigaciones de Crimenes de Alta Tecnologia por sus siglas DICAT de la Policía Nacional, cuenta tambien con la Division de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones por sus siglas DNI, y una Procuraduria Especializada en Delitos de Alta Tecnología del Ministerio Público (PEDATEC).

En Nicaragua, a diferencia de República Dominicana y Costa Rica, no cuenta con un equipo especializado para contrarrestar los ataques cibernéticos, como tampoco cuenta con una estrategia nacional de ciberseguridad, sin embargo posee una legislación que protege los datos personales de sus habitantes, como ser la Ley 787 de Protección de Datos Personales tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa, entre otras leyes que se dedican específicamente a la protección de estos datos. Este país no está adherido a ningún convenio o tratado internacional relacionado con la ciberseguridad, tampoco tiene debidamente tipificados los delitos cibernéticos en una sola legislacion nacional, sin embargo, existen figuras en el Código Penal de Nicaragua que tratan de regular la materia, como ser los artículos 175, 197, 198, 229, 245, 246, 275, 417 del Código Penal nicaraguense.

Por los momentos, Nicaragua no cuenta con Tribunales o agencias especializadas en materia de Ciberseguridad, el ente encargado de investigar los supuestos que suceden en el país es el Ministerio Público, sin embargo es de recalcar que no hay una sección especializada en delitos informáticos.

Por último, en el caso de Honduras que al igual que en Nicaragua, no cuenta con un equipo nacional de Ciberseguridad, que pueda contrarrestar y que defienda a la población de

los ataques de los delincuentes cibernéticos; tampoco cuenta con una política nacional de ciberseguridad que permita asegurar el espacio cibernético del país.

En el sentido de la materia, Honduras se queda corto comparado con sus homólogos países de la región, ya que no cuenta con una legislación vigente que tutele la seguridad informática o los datos personales de sus habitantes, no obstante se encontró que en el año 2015 se sometió a discusión un proyecto de ley de protección de datos personales, el cual se basó en el anteproyecto de ley que fue presentado por el Instituto Nacional de Acceso a la Información Pública en el año 2013; lo último que se conoció fue el debate que se llevó a cabo en abril de 2018, sin embargo este proceso se ha retrasado más de lo esperado ya que el hemiciclo legislativo solo ha aprobado 19 de los 97 artículos que contiene este proyecto.

Actualmente en Honduras, existen artículos en el Código Penal que tienden a proteger a la población de algunos ciberdelitos como ser la suplantación de identidad en el artículo 401, el abuso de dispositivos en el artículo 400, daños a datos y sistemas informáticos en el 399, el acceso no autorizado a sistemas informáticos en el 398, el articulo 592 habla sobre terrorismo electrónico, es de señalar que este no se menciona en el título establecido para los ciberdelitos, sino que se encuentra en el título XXII que habla sobre el terrorismo. Aunado a ello, es de resaltar que Honduras quiso emitir una ley en contra del odio en redes sociales, la Ley de Seguridad y Medidas de Protección ante los actos de Odio y Discriminación en Internet, dicha iniciativa de ley fue discutida por primera vez en el año 2018, actualmente se encuentra detenido dicho proyecto ya que distintos sectores de la sociedad y organizaciones de derechos humanos expusieron su descontento y señalaron que dicha ley constituye una violación a la libertad de expresión; al respecto, el Coordinador de Tecnologías de Información, Jan Alvarado, en una entrevista a Criterio HN (2019) explica que la ciberseguridad son aquellas políticas que deben proteger los dispositivos y la información, pero la ley que se pretende aprobar es una mezcla y una ambigüedad entre políticas de ciberseguridad y censura desde las redes sociales. Lo cual es atentatorio al artículo constitucional número 72, y al artículo 13 de la convención interamericana de los Derechos Humanos.

El país no cuenta con tribunales y agencias de investigación especializadas en materia de ciberseguridad, ni donde promover las denuncias en relación a estos delitos, las cuales actualmente son interpuestas ante el Ministerio Público, en la dependencia de delitos comunes.

Para concluir con el análisis de Honduras, el país no se encuentra adherido a tratados internacionales relacionados con la ciberseguridad, lo cual expertos recomiendan para la adecuada adopción de mecanismos, políticas y legislación en la materia.

Discusión

Importancia de los ciberdelitos en el ordenamiento jurídico hondureño

La falta de legislación en materia de ciberseguridad condiciona a ambigüedades en el cuerpo normativo, en vista que no se está tutelando efectivamente el principio constitucional de la seguridad jurídica de las personas ya que los pocos artículos que regulan los delitos cibernéticos no son claros, dejando en evidencia la necesidad de crear una legislación especial que abarque todos

los ciberdelitos tanto los que incluyen la seguridad de las redes y sistemas informáticos, como también la integridad del sujeto que interactúa a través de estos dispositivos.

Es imprescindible la inclusión del catálogo de ciberdelitos al ordenamiento jurídico hondureño, ya que los pocos artículos que regulan de manera supletoria ante la inexistencia de una legislación especial, dejan de lado conductas que deberían ser reguladas bajo el título de delitos informáticos, como ser el caso de la figura del chantaje que combinado con la extorsión y el requisito sine qua non de que se cometa a través de medios electrónicos, da origen a una nueva conducta que es la sextorsión o extorsión sexual, que como ya se mencionó en párrafos anteriores, no se puede calificar ni con la figura del chantaje ni mucho menos con la figura de la extorsión, dejando en la deriva esta conducta nueva que está afectando el ciberespacio de los Estados, constituyendo una amenaza directa para los jóvenes usuarios de las redes sociales.

Es por ello que hacemos énfasis en la creación de una legislación especial en materia de ciberseguridad, que pueda incluir esta nueva conducta, ya que según una encuesta realizada a jóvenes entre 18 a 24 años, un 72.3% ha sufrido o conoce a alguien que fue perjudicado por un delito cibernético, entre los cuales, se destacaron del resto, la Suplantación de Identidad, que junto con el Ciberbullyng representan un 34.2% de los resultados y la Sextorsión con un 13.1%.

Además, se consultó si habían realizado una denuncia ante las autoridades, la respuesta que se obtuvo fue que NO con un 89.1%, de los cuales solo el 10.9% había realizado efectivamente la denuncia, cifras realmente alarmantes ya que, siguiendo con la encuesta, se concluyó que un 48.5% de las personas desconoce donde interponer la denuncia, el 8.9% no cree que este tipo de conductas sean consideradas delito, el 7.9% dijo que no denunciaba porque tenía vergüenza de lo que pudiera pensar la sociedad de ellos, el 4% dijo tener miedo al agresor, el 30.7% restante no le ha pasado o no cree que la denuncia proceda ante la evidente falta de justicia que existe en el país además de la deficiencia en equipo que carece el Estado.

Estos resultados, dejan en evidencia que uno de los tantos problemas que tiene el Estado en relación a estas conductas nuevas, a través del internet, es la desinformación en la población; no se cuenta con mecanismos adecuados para poder difundir y concientizar la prevención y la denuncia de estos delitos.

Es por ello que resulta necesario la adecuada difusión por parte del Estado de la información de estas conductas, con el objetivo de prevenir y fomentar una cultura de denuncia, donde la víctima tenga confianza y la seguridad de que se le respetarán sus derechos vulnerados, pero para ello requerimos de entes o unidades especializadas y sobre todo, capacitadas en ciberseguridad, pero esto solo se va lograr en un primer punto a través de la cooperación internacional mediante tratados internacionales, como ser la normativa modelo en materia de ciberseguridad que es el Convenio de Budapest, herramienta que proporciona a los Estados mejorar las técnicas de investigación y la armonización en las leyes de los Estados firmantes.

IV. CONCLUSIONES

- Los delitos cibernéticos se pueden considerar delitos trasnacionales, es decir, delitos que cruzan fronteras entre países, en vista de que

en la web no hay un espacio de jurisdicción determinado ya que el delincuente y la víctima pueden estar en diferentes partes del mundo, la cooperación internacional juega un papel fundamental en el espacio cibernético a través de la suscripción de convenios internacionales como ser el Convenio de Budapest y el Llamamiento de París, es así como el Estado de Honduras, garantizaría el bien jurídico principal y fundamental como es la vida, tutelaría la intimidad, la privacidad y el honor y lo referente a los derechos patrimoniales.

- A modo de conclusión, las mujeres representan el mayor número de afectadas por estas conductas delictivas, sin embargo, cualquiera puede ser víctima, debido a que actualmente vivimos en un mundo globalizado donde todos tienen acceso a navegar por la red. Es por ello que es necesario, que el Estado de Honduras adopte en su ordenamiento jurídico estas nuevas figuras que se van fortaleciendo y actualizando con el pasar de los años, por lo cual resulta imprescindible poseer un ordenamiento jurídico acorde a las nuevas conductas delictivas modernizadas.

V. AGRADECIMIENTOS

Agradezco a mi profesora, la Doctora Kenia Paz, por ser guía en este proceso de investigación y proveerme y compartirme sus conocimientos para poder lograr el objetivo de este artículo de investigación jurídica.

VI. BIBLIOGRAFÍA

- Amador, A. (abril de 2021). *La sextorsión como una consecuencia de la suplantación de identidad y la necesidad de tipificarla en el Código Penal Hondureño*. Tegucigalpa, Honduras. Obtenido de https://docs.google.com/spreadsheets/d/1a6hacaDjdlvu0ucL7wa1VQITdARNrb_NkRrVnWmjXZE/edit?resourcekey#gid=1132844360

- Criterio, R. (30 de Octubre de 2019). *Criterio Hn*. Obtenido de https://criterio.hn/ley-de-ciberseguridad-de-honduras-es-ambigua-y-se-enmarca-en-el-odio/

- Europa, C. d. (2001). *Convenio sobre la Ciberdelincuencia*. Convenio sobre la Ciberdelincuencia. Budapest.

- Guevara Yáñez, R. (2019). *El acto de la sextorsion y su necesaria tipificacion en el codigo penal ecuatoriano*. Ambato, Ecuador.

- Rinaldi, P. (27 de abril de 2017). *Le VPN*. Obtenido de https://www.le-vpn.com/es/delito-cibernetico-origen-evolucion/

- RUGAMA., K. S., & ESPINOZA ALGABA, M. J. (2015). *DELITOS INFORMÁTICOS PRESENTES EN LAS REDES SOCIALES EN NICARAGUA Y SU CORRESPONDIENTE APLICACIÓN AL SISTEMA JURÍDICO PENAL*. Obtenido de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/4191/1/230122.pdf

- Sueiras, E. (s.f.). SCRIBD. Recuperado el 14 de marzo de 2021, de https://es.scribd.com/doc/24658747/Redes-sociales-definicion

- Zambrano, A., & Hernández, L. (2020). *Centroamérica Cibersegur*a. IPANDETEC Centroamérica. Obtenido de file:///C:/Users/user/Downloads/CIBERSEGURIDAD_IPANDETEC.pdf