Uniandes EPISTEME. Revista digital de Ciencia, Tecnología e Innovación
ISSN 1390-9150/ Vol. 7 / Nro. Especial / Año. 2020 / pp. 1263-1275

ARTÍCULO CIENTÍFICO
CIENCIAS SOCIALES

Los delitos en la Deep Web y sus efectos sobre las Cibervíctimas frente a la legislación ecuatoriana

Crimes on the deep web and their effects on cyber victims against Ecuadorian legislation

Carrera Calderón, Frankz Alberto[I], Cadena Sayavedra, Hendry Francel [II]; Cepeda Luna, Carlos David [III]; Alvarado Villavicencio, María Soledad [IV]

[I.] ua.frankzcarrera@uniandes.edu.ec, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador
[II.] henrrycadena869@gmail.com, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador
[III.] krlocpda96@hotmail.com, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador
[IV.] solealvi@hotmail.com, Carrera de Derecho, Universidad Regional Autónoma de los Andes, Ambato, Ecuador

Recibido: 01/09/2020
Aprobado: 02/10/2020

RESUMEN

El internet desde su creación se ha vuelto una fuente de información extensa para la sociedad, por lo que desde un inicio se ha necesitado de navegadores, los mismos que buscan dentro de los servidores de la Web, lo que sea que cibernauta este buscando, el problema empieza con la limitación de estos navegadores, limitados a obtener solo información indexada, la misma que es solo una pequeña parte de toda la gran fuente que posee internet. El objetivo general de este trabajo empezó por analizar los delitos que se podrían llevar a cabo mediante el uso de información existente en la Deep web y sus efectos sobre las ciber víctimas. Estos objetivos se lograron mediante la investigación realizada por un método bibliográfico que busco obtener información sobre referente al tema, y luego uso un método analítico – sintético analizando y compactando lo obtenido en cada fuente. Las técnicas usadas en el desarrollo de este trabajo son primeramente la entrevista, practicada a dos profesionales del derecho, y por último una encuesta que ayudo a determinar el conocimiento referente al Tema.

PALABRAS CLAVE: Deep Web; ciber víctimas; Internet; navegadores; investigación.

ABSTRACT

The internet since its creation has become a source of extensive information for society, so from the beginning it has needed browsers, the same ones that search within the servers of the Web, whatever cybernaut is looking for, the problem starts with the limitation of these browsers, limited to obtaining only indexed information, the same that is only a small part of the whole large source that has the internet. The overall objective of this work began by analyzing the crimes that could be carried out by using existing information on the Deep Web and its effects on cyber victims. These objectives were achieved through research conducted by a bibliographic method that Sought to obtain information on the subject, and then use an analytical – synthetic method by analyzing and compacting what is obtained in each source. The techniques used in the development of this work are first the interview, practiced to two professionals' law, and finally a survey that helped determine knowledge regarding the subject.
KEYWORDS: Deep network; cyber victims; Internet; browsers; investigation.

INTRODUCCIÓN

El uso de Internet se ha generalizado a nivel mundial, más aún en estos días en los cuales por motivos de la pandemia del Covid19, las personas han tenido que permanecer mucho tiempo en sus casas.

Los usuarios de Internet al momento de escribir este artículo sobrepasan los 4.600 millones, esto equivale a decir que más de la mitad de las personas en el mundo son usuarios de esta tecnología, de igual forma hay más de 1.700 millones de sitios web, otro aspecto significativo que debe destacarse es que en un día hay más de 5.000 millones de búsquedas usando Google (Internet Live Stat, 2020). En Ecuador para el año 2016 había 7'055,575 usuarios de Internet, alcanzando el 43% de su población (Internet Live Stat, 2020).

Las personas usan Internet para una gran cantidad de actividades, una de las más destacadas es trabajar con los datos existente en la red, estos datos han sido almacenados en computadoras especiales denominadas "servidores" los mismos que se encuentran en todo el mundo. De ahí que, se han creado aplicaciones llamadas "motores de búsqueda", las mismas que proporciona a sus usuarios una manera fácil de acceder a la información en Internet, realizando un proceso llamado indexación. Uno de los motores de búsqueda más conocidos es Google, pero no es el único. Según worldwidewebsize (2020), hay más de 5.000 millones de páginas web indexadas en Google. De igual forma "en 2010, de una estimación de 5 millones de Terabytes, Google sólo había indexado un 0,004% y la cantidad de datos que se almacena en Internet es cerca de 1 Zettabyte (1.099.511.627.776 gigas)" (xataka, 2016).

Como se mencionó anteriormente una pequeña porción de páginas web están indexadas, eso quiere decir, que se encuentran organizadas como en un libro de páginas amarillas para encontrarlas de forma rápida y sencilla. El resto de las páginas web que no están en dicha indexación es conocido como Deep Web o web profunda, además la web "no es solo a lo que podemos acceder mediante un navegador" (Casas-Herrer, 2017, pág. 21).

De ahí que se puede hablar de una web normal y una profunda (Allegritti, 2015), en este trabajo se aborda la Deep Web o Web Profunda, teniendo en cuenta dos aspectos de esta tecnología, por un lado, debido a la gran cantidad de datos que se encuentran en dicha red, es muy probable que en la misma existan páginas web que publiquen información que pudieran ser considerada delito o que permitieran el cometimiento de un delito. Por otro lado, tomando en cuenta los pilares sobre los cuales descansa la Deep Web (anonimato, la criptografía profunda, información no detectable, no fiscalización, alienación, entre otros) muchos cibercriminales acceden a esta red para llevar a cabo sus actividades.

Según Davara-Rodríguez (2010) en su "Manual de Derecho Informático", define al delito informático como una acción que por sus características ilícitas se le ubica dentro del concepto de delito, esta acción es llevada a cabo utilizando un medio informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Los objetivos propuestos en la investigación fueron: fundamentar teóricamente los principios que rigen la Deep web, sus componentes, causas y las ciber-victimas; desarrollar un análisis entre los delitos que se puedan cometer utilizando la información publicada en la Deep web y normas jurídicas ecuatorianas; finalmente determinar el nivel de conocimiento sobre la Deep Web y delitos informáticos en la carrera de Derecho UNIANDES Ambato Segundo y Tercer Nivel presencial.

MÉTODOS

La parte inicial del trabajo se centra en los principios que rigen a la Deep Web, con el fin de tener claro el funcionamiento de la misma y su estructura, lo cual permitió tener una idea de las actividades ilícitas que podrían ejecutarse en su interior. Para ello se realizó una investigación documental expositiva, las principales fuentes de acceso a la información fueron: artículos científicos, libros especializados y sitios web técnicos.

Para el desarrollo de la siguiente etapa de la investigación se utilizó el método analítico-sintético, el mismo que permitió llevar a cabo un análisis comparativo entre los posibles delitos (infracción penal) que se podrían llevar a cabo en la deep web y nuestro Código Orgánico Integral Penal (COIP, 2014), para establecer si los mismos son sancionados por nuestra legislación. Finalmente, se aplicó 37 encuestas con 11 preguntas a los estudiantes de

segundo y tercer nivel de la Carrea de Derecho de segundo y tercer nivel de UNIANDES utilizando Microsoft 365 Forms y entrevistas a dos profesionales del derecho.

RESULTADOS

1. Análisis teórico de la Deep Web: concepto, características y fundamentación.

La Deep Web puede ser entendida como un conjunto de archivos y paginas dentro de Internet que no están indexadas por los navegadores comunes, como es el caso de Google (Ibáñez, 2017). Indexar en forma general puede ser entendida como un proceso que permite organizar de manera ordenada datos e información, como un índice para que dicha información sea fácil de encontrar dentro internet por parte de los navegadores que buscan información en la misma.

El termino Deep Web traducido al español significa “Internet Profunda” debido a la información que contiene y la complejidad del acceso a esta tecnología; el anonimato de las personas que navegan en esta red es uno de sus pilares de funcionamiento y “uno de los principales problemas para las diferentes fuerzas y cuerpos de seguridad de un país a la hora de investigar posibles delitos cometidos por los ciberdelincuentes” (Yuste, 2015).

Para acceder a la Deep web es necesario un conjunto de programas (software) especializados, de acuerdo con Díaz (2017), el uso de estos en países como Arabia Saudí, Austria, China, Egipto, Irán, Rusia es considerado un hecho delictivo. Pero en la mayoría de los países a nivel mundial es legal descargar, instalar y/o utilizar software que permita el acceso a la Deep web.

Debido a la cantidad de información sensible, a la Deep Web se le puede comparar con un mercado negro, ya que esta atrae la atención de personas que no siempre tienen buenas intenciones, sacado a relucir la parte más oscura del ser humano, que se aprovecha del anonimato existente dentro de los varios niveles de la Deep Web, llegando a encontrar pornografía infantil, incluso terrorismo o secretos de estado en los niveles más profundos. Hay que tomar en cuenta que el Internet en general permite la transmisión y distribución de forma instantánea de cualquier tipo de dato de forma relativamente sencilla en relación con otros medios de comunicación (Cohen-Almagor, 2013).

Deep Web, Dark Web y Dark Net.

Deep Web, Dark Web y Dark Net, son términos que a simple vista pueden ser tomados como sinónimos, pero realmente son diferentes; la figura 1 muestra un organizador gráfico simple, el cual es conocido como Iceberg.

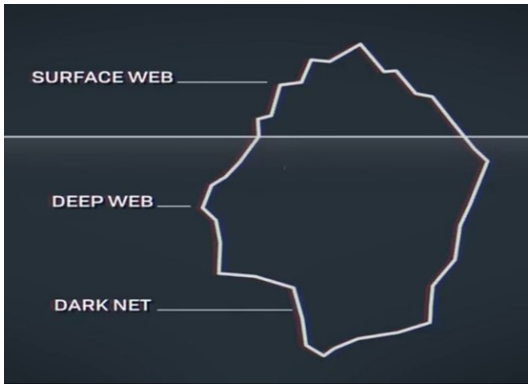

Figura 1. Iceberg de la web.
Tomado de (xataka, 2016)

La pequeña punta de este esquema es la Surface Web o Web Normal, donde comúnmente todos acceden, luego por debajo se encuentra la Deep Web, que son los primeros e intermedios niveles de la Internet Profunda, y por último a la parte más profunda de la red se tiene a la Dark Net, el lugar más difícil de acceder.

Surface Web, es el internet que comúnmente es utilizado de manera general, conformando esta un 4% apenas de toda la información existente en la web. Este nivel de internet es el que todos conocen, en el que podemos encontrar redes sociales o navegadores académicos, que son utilizados con gran facilidad. En la Surface web el navegar es rastreable, mediante el IP de quien acceda a esta, y según Live Stats (2020), la Surface Web está integrada por acerca de 1.139 millones de páginas web.

Deep Web, es lo opuesto a la primera ya que es el contenido que no se encuentra indexado, englobando así toda la información que se encuentra online dentro de internet, pero no se encuentra publica a diferencia de la información que se encuentra en la Surface Web, ya que los navegadores comunes no captan información de esta. Como ejemplo de sitios que se pueden encontrar dentro de la Deep Web, son las paginas ordinarias pero que se encuentran bajo protección de alguna “barrera de pago” (Paywall), o incluso los archivos de Dropbox mejor resguardados. Según estadísticas el contenido de la Deep Web resulta un 90% de la internet.

La Dark Web pertenece a la Deep Web, pero no significa lo mismo, ya que no contienen la misma información ni facilidad de acceso. Como Dark Web (Web Oscura) tenemos a una pequeña parte a la que solo se puede acceder con el uso de aplicaciones específicas tras un proceso que no es sencillo. Como un ejemplo de estas aplicaciones se puede mencionar a Tor, el cual es una especie de navegador especifico, que, a comparación con los ordinarios, este es un poco más lento por su función de mantener el anonimato y acceder a diferentes sitios de difícil o riesgoso acceso. Dentro de esta web se puede encontrar información que ha sido intencionalmente oculta en estos sitios, debido a su contenido, dando origen al nombre de esta Web, ya que la mayoría de este tipo de información es de índole negativa o secreta.

Como Dark Net, se puede entender al conjunto de redes específicas, las cuales guardan paginas o contenido de la Deep Web. Como estas redes se puede mencionar a TOR, FreeNet, I2P. o Invisible Internet Project. Entonces la Dark Net está conformada por gran cantidad de Dark Webs, que almacenan información con contenido violento o escandaloso, que normalmente inflige la ley, por lo que se encuentra dentro de este lugar.

Origen de la Deep web.

El concepto Deep Web o Web Invisible fue dado por primera vez en 1994, cuando Mike Bergman realizó la publicación de un artículo en *Journal of Electronic*, dicho artículo se refería a las webs que no se encontraban anexadas a los navegadores ordinarios, webs ocultas.

Muchas de estas webs ocultas surgieron por la necesidad de defensa de los internautas en relación a la vigilancia que tanto países como organización realizan sobre la navegación en la red, considerado como “una amenaza para la libertad y privacidad de las personas” (Cohen-Almagor, 2013). De ahí que se desarrolló tecnología para garantizar el anonimato de los usuarios al momento de navegar por Internet.

Básicamente se “trata de dificultar el establecimiento de la relación con el punto de acceso desde el que se navega, gracias al empleo de técnicas de criptografía en una estructura multicapa (cebolla) y al uso de distintos equipos para deslocalizar a emisor y receptor. De esta manera, la dirección IP permanecerá oculta, lo cual impide conocer la geolocalización de sus usuarios, así como conocer las páginas que han visitado” (Soldino & Guardiola, 2017, pág. 20).

Ingresando a la Internet Profunda.

Al tratarse de un nivel menos accesible que la internet ordinaria, se requiere la ayuda de otro tipo de navegadores que forman parte de programas especializados para este tipo de búsquedas, en el caso de la Deep web, la herramienta más usada para navegar en la misma es TOR (The Onion Rourter), la cual fue creada en el 2002 por Roger Dinglendine, Nick Mathewson y Paul Syverson, a partir del proyecto desarrollado por el Laboratorio Naval de los Estados Unidos (Yuste, 2015) y el objetivo de este programa es otorgar anonimato y privacidad a sus usuarios mientras navegan por Internet. Tor es un programa que permite a su usuario navegar de manera anónima y encriptada. Usando el anonimato que brinda el software Tor dentro de la Deep web se han podido desarrollar varias fuentes de información, comunidades de extrema disidencia política, incluso han llegado a desarrollarse los hackers, dando origen al delito informático, y varias conductas antijuridicas dentro de la internet profunda.

Tor es una herramienta tecnología que brinda un servicio online, el cual permite al usuario conectarse a una red de comunicaciones dentro de la Internet bajo anonimato, pero a

comparación con un navegador convencional de la Internet visible, Tor tiende a demorarse un poco más debido al proceso que lleva para buscar dentro de la Web.

Lo oscuro de la Deep web

Como se dijo anteriormente, la información en la Deep web es muy variada y por lo cual puede ser usada de varias formas, según el criterio de Gay Fernández (2015) esta alberga servicios de:

> Venta de drogas, venta de armas, blanqueo de dinero, contratación de mercenarios, documentos científicos, venta de objetos robados y billetes falsos, información bursátil confidencial, turismo sexual y prostitución, pornografía infantil y bizarra, vídeos gore y de violencia extrema, manuales de terrorismo, instrucciones para fabricar artefactos explosivos, tráfico de animales exóticos, claves de identificación para sitios como PayPal, eBay o Skype, literatura conspiranoica, documentos de secreto de Estado (pág. 12).

En Ecuador el Código Orgánico Integral Penal (COIP), sanciona una serie de actividades o conductas delictivas que se realizan utilizando medios electrónicos, mismos que se analizan en este trabajo (Sánchez Insuasti, 2017).

Cibervíctimas

Para empezar hablar sobre las ciber victimas es importante tener en cuenta, que las víctimas y el comportamiento que tiene cada uno de ellas son elementos determinantes, por los factores y los acontecimientos que se suscitaron para que el delito se haya cometido y que la persona haya quedado vulnerable ante sus derechos, en el ciberespacio la victima juega incluso un papel condicionante aún mayor, en el sentido de definir el ámbito de oportunidad criminal, ya que la persona por si sola ubica a simple vista sus datos personales, sus actividades cotidianas, de igual forma su entorno familiar queda muy expuesto ya que generalmente se publica fotos familiares, y eso ya les convierte en víctimas, de igual forma se le da paso a la persona que comete el cibercrimen a movimientos económicos, y si bien es cierto no existe un control mayor para cada una de las páginas que las personas navegan a diario, es por ello que es fundamental mencionar que la mayor parte donde podemos observar que existe un índice alto en cibercrimen son las redes sociales, ya que a cada persona se la deja vulnerable hacia los ataques, puede ser una persona que su edad no es real, y cometa algún tipo de delito que se suele llamar «grooming», o de igual forma no tienen en consideración ubicar su contenido en privado y la mayoría de las personas las puede observar. Los incidentes en Internet suelen ser asociados con el nivel de seguridad informática que poseen las empresas o corporaciones atacadas, esto pues genera un desprestigio en la empresa atacada, descrédito de fiabilidad de la gestión propia de la empresa. . Se puede señalar que los mismos medios tecnológicos son los causantes del ciberbullying,

ya que si bien es cierto se puede ocasionar inconvenientes entre los jóvenes, que muchas veces la ciber víctima lo conduce al suicidio.

El ciberacoso puede estar presentado como un problema en la salud pública dada su incidencia y afectación hacia las personas convirtiéndolas en ciber víctimas y todos los riesgos que esto conlleva, es decir que se tiene que tener muy presente el tipo de víctima y como lo afecta, las ciber víctimas y los ciberacosadores presentan perfiles similares en cuanto a determinados rasgos de personalidad, es decir que pueden presentar cuadros de inestabilidad emocional, autoestima baja y a la vez cuadros psicopatológicos.

Debe tenerse claro que el simple hecho de que a una persona se le haya considerado ciber víctima, no está teniendo el adecuado acceso hacia una vida digna, ya que esta fue vulnerada de sus derechos y de igual forma se hayan violado muchos de sus derechos, se puede mencionar, que usualmente las víctimas o ciber víctimas no lo hablan pues prefieren quedarse en silencio por el temor de que algo malo les vaya a pasar a ellos o incluso a su familia, puesto que su agresor o ciber agresor impone amenazas contra estas personas que si bien es cierto no sabemos si pueden ser ciertas o no, es por ello que es muy importante tener en cuenta que el acceso al Internet no es cualquier cosa.

2. Análisis entre delitos y norma jurídica ecuatoriana.

Uno de los resultados más generados por la investigación fue el análisis entre delitos y normativa jurídica ecuatoriana, la misma se encuentra detallada en la tabla 1.

Tabla 1. Delitos relacionados con la Deep web según el C.O.I.P.

Tipo penal	Presunto delito	Artículo	Bien jurídico protegido	Verbo rector	Circunstancia	Sanción: Pena privativa de libertad
Publicidad de tráfico de órganos	Comercialización Ilegal de órganos humanos (hígado, riñón)	Art. 97.-	Integridad física la vida	Promueva, favorezca, facilite o publicite la oferta, la obtención	El tráfico ilegal de órganos y tejidos humanos o el trasplante de los mismos.	De siete a diez años.
Comercialización de pornografía con utilización de niñas, niños o adolescentes	Contenido o redes de pederastas que venden y dan promoción sus videos	Art. 104.-	Integridad sexual	publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda,	Para uso personal o para intercambio.	De diez a trece años
Instigación al suicidio	Videos snaf: Contenido no censurado donde se visualiza: Torturas Mutilaciones	Art. 154.1 .-	Integridad física La vida	induzca o dirija mediante amenazas, consejos, órdenes concretas, retos	provoque daño así mismo o ponga fin a su vida	De uno a tres años

	Asesinatos.					
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	Conversaciones con fines pornográficos con pedófilos u otros interesados.	Art. 173.-	Derechos humanos, libertad sexual, integridad sexual	Proponga concertar un encuentro	Atreves de un medio electrónico o telemático con finalidad sexual o erótica	De uno a tres años
Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	Oferta de servicios sexuales a los denominados pedófilos o a cualquier interesado.	Art. 174.-	Derechos humanos, libertad sexual, integridad sexual	utilice o facilite	para ofrecer servicios sexuales con menores de dieciocho años	De siete a diez años.
Estafa	El CARDING Venta de tarjetas de crédito clonadas o los datos de la persona titular para compras online.	Art. 186.-	Propiedad privada	la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos	realice un acto que perjudique su patrimonio o el de una tercera,	De cinco a diez años. 7 a 10 años si supera 50 SBU.
Apropiación fraudulenta por medios electrónicos	La persona quién hackea, Información privada para su beneficio u oferta en la web profunda.	Art. 190.-	Propiedad privada	alterando, manipulando o modificando	facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes.	De uno a tres años.
Organización o financiamiento para la producción o tráfico ilícitos de sustancias catalogadas sujetas a fiscalización	Tráfico ilegal de drogas baratas: Canabis Cocaína. Éxtasis Mezcalina. Heroína. En un gran mercado negro.	Art. 220.-	Buen Vivir	Trafique, sea que oferte, almacene, intermedie, distribuya, compre, venda, envíe, transporte, importe, exporte, tenga o posea	comercializar o efectué tráfico ilícito de sustancias estupefacientes y psicotrópicas.	-Mínima 1 a 3 años. -Mediana, de 3 a 5 años. -Alta, de 5 a 7años. -Gran escala, de 10 a 13 años.
Tráfico ilícito de armas de fuego, armas químicas, nucleares o biológicas.	Venta y publicación ilícita de de una variedad de armas a bajo precio. Que llega anónimamente a las casas.	Art. 362	Seguridad Publica	desarrolle, produzca, fabrique, emplee, adquiera, posea, distribuya, almacene, conserve, transporte, transite, importe, exporte, reexporte, comercialice.	Sin autorización de la autoridad competente,	De cinco a siete años

3. Investigación de campo

Encuesta.

Se aplicó una encuesta estructurada por 11 incisos, mediante la plataforma Microsoft 365 Forms a estudiantes de segundo y tercer semestre de la carrera Derecho de la Universidad UNIANDES Ambato, obteniendo un resultado de 37 respuestas.

Como resultado de dicha investigación se estableció que el navegador más usado por los estudiantes era Google Chrome y apenas un 2% usa o usó TOR.

El 60% de los encuestados navega en promedio más de 3 horas al día y solo el 2% lo utiliza menos de 30 minutos.

El dispositivo físico más usado para navegar por internet es el celular con un 49%, le sigue el uso de laptops con un 43%, nadie usa tabletas y solo un 8% usa computadoras de escritorio.

En referencia al motor de búsqueda utilizado todos los estudiantes trabajan con Google, nadie utiliza otros motores como Bing, Ask, Yahoo u otros.

Los estudiantes en relación a la seguridad al navegar consideran que su equipo por si solo puede protegerles en un 64%, un 21% utilizan algún software protección como antivirus, pero un 15% no hacen nada ni les interesa el tema.

Referente al conocimiento que tienen sobre la Deep Web, los encuestados en un 68% tiene la idea clara de lo que es dicha red, mientras que el 27% no tiene idea de lo que es esta tecnología y un 5% creen que es un sitio de compras o una red social.

Al preguntar sobre los peligros que conlleva navegar en internet la mayoría considera que el mayor peligro es el robo de información con un 54%, ser víctima de estafa un 20%, plagio de identidad un 2%, vulneración de cunetas privadas un 10%, secuestro un 2%, trata de personas un 2% y acoso un 10%.

El 29,7% de encuestados consideran que tanto el COIP, Ley de Comunicaciones, Ley de comercio electrónico, firmas electrónicas y mensaje de datos tiene relación a los delitos utilizando medios informáticos y apenas 1 personas manifestó que el COGEP y 2 personas dijeron que ninguna ley.

Los estudiantes al preguntarles sobre si algún momento han utilizado la Deep web dijeron en un 86% que nunca lo han hecho, pero un 14% es decir 5 personas si lo habían realizado.

Al preguntar sobre la importancia de la seguridad informática la mayoría respondió era por el uso masivo de esta tecnología, ningún encuestado respondió diciendo que no era importante la seguridad informática.

Entrevista

Para la entrevista se usó una guía de entrevista como instrumento, la cual consta de seis preguntas: 1) ¿Qué es un delito cibernético y cuando se configuraría uno de ellos en la web profunda?; 2) su postura del uso de las TIC y la información que se puede encontrar en la web

profunda; 3) de acuerdo con su criterio cual es la posición se encuentra frente a estos delitos informáticos en relación a otros países. (convenio de Budapest); 4) según el COIP ¿cuáles son las consecuencias jurídicas que están generando los ciberdelincuentes. (Penas y sanciones de acuerdo con las normas tradicionales) ?; 5) en el caso de presentarse un delito informático como sería el proceso a seguir y los órganos competentes para conocer los presuntos delitos. (ante quien puede denunciar, quien se encarga, como interviene fiscalía);6) ¿qué hacen las autoridades para controlar o monitorear estas conductas. (si existe una unidad especializada, etc.)?

Los entrevistados mostraron en sus respuestas el conocimiento que tenían sobre el tema y su posición frente al uso de la tecnología de la información y la comunicación, de igual manera se establecieron los pro y contras de nuestra legislación en el tema de los ciberdelitos y la Deep web.

DISCUSIÓN

El objetivo principal de este trabajo fue tratar de determinar posibles delitos cometidos mediante el uso indebido de la Deep, lo que hizo que sea necesario en primer momento indagar varias fuentes bibliográficas primarias y secundarias de información, dando como resultado un concepto entendible sobre Deep Web, y sobre todo una tabla que compara los posibles delitos informáticos que se pueden llevar a cabo mal de forma inadecuada la Deep Web en relación con la normativa vigente del Ecuador, dando así un panorama que ayuda a apreciar las conductas antijuridicas resaltantes dentro del internet, ya que como tal el navegar dentro de la Web, no es ningún delito, ni siquiera la Deep Web es ilícita, porque la misma comprende toda la información existente dentro de la internet.

El resultado más favorable de este trabajo se evidencia dentro de la tabla 1, porque se puede apreciar como tal los posibles delitos comparados con normativa referente, la misma que se encuentra vigente. Fue necesario generar y aplicar una encuesta que permita evaluar el nivel de conocimiento de los estudiantes de Derecho sobre la Deep Web, posiblemente esta herramienta debe ser mejorada, pero de acuerdo a los autores de la investigación las 37 respuestas por parte de estudiantes de 2 y 3 nivel de la Carrera de Derecho; no se pudo cubrir con la cantidad deseada de estudiantes debido a que se la aplico usando Microsoft Forms y la respuesta a la misma dependía del deseo de aplicarla o no de los estudiantes. Como segundo resultado se obtuvo una orientación dentro del tema de ciberdelito desde un punto de vista jurídico, usando la entrevista a profesionales del Derecho, de los cuales principalmente se desea conocer su punto de vista jurídico sobre el tema de estudio.

CONCLUSIONES

La Deep Web está conformada prácticamente por el 90% de la información existente dentro de internet, misma que no fue creada con fines ilícitos, sino por lo general es utilizado por las varias personas, debido a sus características de anonimato dentro de la Internet. TOR, es una aplicación, que, si se lo usa con buena disposición y sobre todo con precaución, sería una herramienta que puede resultar fundamental para desarrollos científicos por su capacidad de buscar información.

Se puede establecer que los factores en los cuales las ciber víctimas se ven afectadas en la mayoría es la no supervisión y el no control por parte de los padres hacia los adolescente y si bien es cierto recae una responsabilidad absoluta en los adultos ya que se están vulnerando derechos de las personas al quedar indefensas, muchas veces por miedo de los ciber agresores, el Ecuador no cuenta con medidas sancionatorias para los ciber agresores o el grooming es por ello se debe estar conscientes del daño y precaución al momento de navegar por el internet o por las redes sociales y seguir las recomendaciones .

Es muy difícil combatir a los delitos que ocurren en la web profunda, por el tema de la jurisdicción, Ecuador únicamente conoce infracciones en el marco de territorio pues esos delitos se pueden configurar en cualquier parte del mundo, dificultando la búsqueda del presunto infractor o de la dirección de los sitios webs donde se ofrecen cosas ilícitas.

La investigación no trata de incitar que ingresen a la Deep web, puesto que si bien es cierto no es un delito la acción navegar en ella, su acceso representaría un gran peligro, ya que, al interactuar con todo tipo de hackers, puede darse el caso que se descubra la identidad de quien está navegando y sea víctima de cualquier ciberdelito.

No todos los países tienen en sus legislaciones una ley específica que regule los delitos asociados a las nuevas tecnologías, como el caso del Ecuador. Por consiguiente, no forma parte del convenio de Budapest, pues precisamente el país miembro debe tener una ley de delitos informáticos que se adapten a este convenio.

REFERENCIAS

Allegritti, P. (2015). *Deep Web la parte oscuera y peligro del Internet.* House grupo editorial.

Alonso, C., & Romero Triñanes, E. (2016). *Dialnet*. Obtenido de Ciberacoso: Características de personalidad y psicopatológicas del ciberagresor y de la cibervíctima: https://dialnet.unirioja.es/servlet/articulo?codigo=5984912

Casas-Herrer, E. (2017). *La red oscura: En las sombras de Internet: el cibermiedo y la persecución de lo delitos tecnológicos.*

Cohen-Almagor, R. (2013). Online chid sex offenders: challenges and counter-measures. *The Howard Journal of criminal justice*, 190-215.

COIP. (2014). *Código Orgánico Integral Penal.* Quito: ECP.

Díaz, M. (30 de agosto de 2017). *https://clickjuridico.es.* Obtenido de https://clickjuridico.es/es-legal-navegar-por-la-deep-web/

Gay Fernández, J. (2015). *La deep web: el mrcado ngro global.* Sevilla: Universidad de Sevilla.

Ibáñez, ,. E. (2017). *Dark web y deep web como fuentes de ciberinteligencia utilizando minería de datos.* Tercera Epoca.

Internet Live Stat. (03 de 08 de 2020). *https://www.internetlivestats.com/*. Obtenido de https://www.internetlivestats.com/

Miro Llinares, F. (2012). *El cibercrimen.* Madrid: Marcial Pons.

Ortega Baron, J., Torralba, E., & Buelga , S. (2017). *Revista de Estudios e investigación en Psicología y Educación*. Obtenido de Distrés psicológico en adolescentes víctimas de cyberbullying: https://www.uv.es/lisis/jessica/2017/5art-reipe.pdf

Perez Machio, A. I., & De la Cuesta Arzamendi, J. L. (s.f.). *Ciberdelincuentes y Cibervíctimas.* Obtenido de https://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf

Perrino, I. L. (2018). Un paseo por la Deep Web.

Sánchez Insuasti, S. (2017). *Temas Penales III.* Quito: Corte Nacional de Justicia.

Soldino, V., & Guardiola, J. (2017). Pornografía infantil: cambios en las formas de obtención y distribución. *Revista Electrónica de Ciencia Penal y Criminología* , 19-28.

WWWS. (03 de 08 de 2020). *https://www.worldwidewebsize.com/*. Obtenido de https://www.worldwidewebsize.com/

xataka. (28 de 11 de 2016). *https://www.xataka.com*. Obtenido de https://www.xataka.com/tecnologiazen/sabemos-cuanto-ocupa-todo-el-contenido-que-hay-en-internet-en-este-momento

Yuste, C. (2015). Deep web y monedas virtuales: entorno priviligiado para actividades terroristas. *UNIR*.