Universidad Nacional de Loja

Facultad Jurídica Social Administrativa

Carrera de Derecho

Incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso

Trabajo de Integración Curricular previo a la obtención del Título de Abogado

AUTOR:

Miguel Angel Benitez Guayllas.

DIRECTOR:

Dr. Freddy Ricardo Yamunaqué Vite, Mg. Sc.

LOJA - ECUADOR

2024

Certificación

Loja, 01 de marzo del 2023

Dr. Freddy Ricardo Yamunaque Vite Mg. Sc

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

C E R T I F I C O:

Que he revisado y orientado todo el proceso de elaboración del Trabajo de Integración Curricular denominado: "**Incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso"**, previo a la obtención del título de **Abogado,** de autoría del estudiante **Miguel Angel Benitez Guayllas**, con cédula de identidad Nro.**1150751855**, una vez que el trabajo cumple con todos los requisitos exigidos porla Universidad Nacional de Loja, para el efecto, autorizo la presentación del mismo para su respectiva sustentación y defensa.

Dr. Freddy Ricardo Yamunaque Vite Mg. Sc.

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Autoría

Yo, **Miguel Angel Benitez Guayllas**, declaro ser autor del presente Trabajo de Integración Curricular y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido del mismo.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de mi Trabajo de Integración Curricular en el Repositorio Digital Institucional - Biblioteca Virtual.

Firma: 

Cedula de identidad: 1150751855

Fecha: Loja, 09 de enero de 2024.

Correo Electrónico: miguel.benitez@unl.edu.ec

Teléfono: 0992260231

Carta de autorización por parte del autor, para la consulta, reproducción parcial o total y/o publicación electrónica del texto completo del Trabajo de Integración Curricular

Yo, **Miguel Angel Benitez Guayllas**, declaro ser autor del Trabajo de Integración Curricular denominado: "**Incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso",** como requisito para optar al título de **Abogado**, autorizo al sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre la producción intelectual de la Universidad, a través de la visibilidad de su contenido en el Repositorio Institucional.

Los usuarios pueden consultar el contenido de este trabajo en el Repositorio Institucional, en las redes de información del país y del exterior con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia del Trabajo de Integración Curricular que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 09 días del mes de enero de dos mil veinticuatro.

Firma: 

Autor: Miguel Angel Benitez Guayllas.

Cédula: 1150751855

Dirección: Loja, Juan José Samaniego y Ramon Pinto.

Correo electrónico: miguel.benitez@unl.edu.ec

Teléfono: 0992260231

DATOS COMPLEMENTARIOS

Director del Trabajo de Integración Curricular: Dr. Freddy Ricardo Yamunaque Vite, Mg. Sc.

Dedicatoria

El presente trabajo de integración curricular se lo dedico a mis padres, Rosa Guayllas y Angel Benitez, por haberme apoyado en el transcurso de mis años de formación académica a su vez por ser el ejemplo que todo hijo deseara tener.

A mis hermanos, que con el pasar de los años se vuelven una parte muy importante en mi vida, y han sido la principal razón del porque sigo estudiando.

Finalmente, agradezco a mis amigos, pero en especial a David, Cristian, Ximena y Angie por hacer mi estadía en la universidad una experiencia amena.

Miguel Angel Benitez Guayllas.

Agradecimiento

Agradezco a la Universidad Nacional de Loja por tener los lineamientos adecuados para la formación de un profesional en la carrera Derecho en la facultad jurídica, social y administrativa, ya que sus componentes teórico - prácticos, han generado una mayor concentración e interés por la carrera.

De igual manera, extiendo mi agradecimiento a aquellos docentes de la carrera en las áreas de Derecho Penal y Civil, y en especial a mi director que no solo fue una persona que dirigió el presente trabajo, también fue un amigo para mí.

Miguel Angel Benitez Guayllas.

Índice de Contenidos

Índice de Tablas

Índice de Figuras

Índice de Anexos

1. Título

Incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso.

2. Resumen

El derecho penal nace como una opción de control social con la finalidad de proteger a la sociedad de los delitos y la violencia y a su vez establecer un sistema de justicia que sanciones a aquellos que han cometido delitos y proteja los derechos de las víctimas, siendo así que se da la creación de un conjunto de reglas y normas que regulen las conductas humanas y prevengan y sancionen aquellas que se consideren dañinas. Pero esto en la actualidad con el avance de la sociedad el derecho penal también se adapta a las conductas humanas llevando a si a un nuevo derecho penal denominado derecho penal en el ciberespacio, este concepto parte de una historia que actualmente es vivida dando así a nuevos problemas de los cuales se abarca en este proyecto ,como lo es el ciberstalking, entonces para entenderlo mejor el derecho penal en el ciberespacio se lo dice como aquel conjunto de leyes y normas que regulan y sancionan los delitos cometidos a través de la tecnología y redes informáticas el mismo que abarca un amplio rango de delitos.

Pero esto es solo el inicio de la conceptualización de un derecho penal cibernético, la creación del mismo da paso a temas bastante interesantes como lo es la persona digital la cual es la base misma o fuente de información que usa el delincuente informático para el cometimiento de sus actuaciones.

A partir de lo anterior, el trabajo plantea un estudio doctrinario de la figura delictiva denominada “ciberstalking” por lo que se realizara precisiones conceptuales acerca de su definición y definiciones a la vez que trataremos de explicar la dificultad que presenta esta nueva era digital.

Para llevar a cabo el objetivo, el estudio se ha estructurado en dos apartados, en primera instancia se define la base que es el derecho penal y por ende el derecho penal en el mundo digital dando así paso a sus nuevos conceptos que nos trae está era como lo es los nuevos problemas de perseguibilidad y también una forma de combatir a los mismos y una vez conceptualizados los preceptos necesarios para el entendimiento se dará el análisis de la figura delictiva que es tema de estudio que se lo llama el “ciberstalking” en el mismo que se analizaran sus elementos y características constitutivos. En segunda instancia son las encuestas, entrevistas que junto a la reforma jurídica nos dan la información necesaria para verificar la existencia de esta conducta delictiva en la sociedad ecuatoriana y con la reforma jurídica trataremos de dar una sanción a dicha conducta,

Se prima el efecto de la investigación, con el método descriptivo, inductivo, deductivo y estadístico que permiten ejecutar de manera adecuada el análisis de un enfoque basado en mejorar el concepto y persecución del delincuente cibernético y por ende el estudio de la figura delictiva denominada “Ciberstalking”

De igual manera, los resultados de este estudio académico evidencian una falta de normativa para la correcta sanción de esta conducta.

Palabras clave: Ciberstalking, persona digital, Derecho penal en el ciberespacio, anonimato.

2.1.Abstract

Criminal law was created as an option for social control in order to protect society from crime and violence, establishing a justice system that penalizes those who have committed crimes and protects the victims' rights creating a set of rules and regulations that control human behavior, prevent and punish those that are considered harmful. Currently, with the advancement of society, the law also adapts to human behavior, leading to a new legislation called criminal law in cyberspace. This concept is based on current experiences which create problems that are analyzed in this project, such as "cyber-stalking". In order to better understand criminal law in cyberspace, it is considered as that set of laws and regulations that control and punish crimes committed through technology and computer networks, which covers a wide range of felonies. This is just the cornerstone of the cybernetic criminal law conceptualization. Its creation makes way to quite interesting topics such as the digital person, which is the very base or source of information used by the computer criminal to commit their actions.

Considering the aforementioned, this research work suggests a doctrinal study of the criminal figure called "cyber-stalking"; furthermore, conceptual clarifications will be made about its definition while trying to explain the difficulty presented by this new digital era.

In order to fulfill the goal, the study has been structured in two sections: first, the criminal law is defined as well as the criminal law in the digital world, giving way to these new era's concepts, for instance the new prosecution problems and also a way to fight them. Once the most important notions have been defined, the analysis of the criminal figure called "cyber-stalking" will be carried out describing its main features. Then, surveys, interviews along with the legal reform will provide the information needed to verify the existence of this criminal behavior in Ecuadorian society; in addition, use a legal reform to penalize this conduct.

The result of the investigation is supported by the descriptive, inductive, deductive and statistical methods that allow to adequately execute the analysis of an approach based on improving the concept and prosecution of a cybercriminal and therefore the study of the criminal figure called "cyber-stalking"

Similarly, the results of this academic study show there are not enough regulations to correctly penalize this conduct.

Keywords: cyber-stalking, digital person, criminal law in cyberspace, anonymity.

3. Introducción

El tema a tratar versa de la figura delictiva llamada "ciberstalking" el mismo que parte dos palabras que son ciber y stalking, dando así un concepto nuevo el mismo que decimos que este es una forma de acoso dado en las redes sociales o cualquier otro medio que conecten a más cibernautas dando así paso a una conducta con un comportamiento repetitivo y no deseado que se realiza a través de internet o dispositivos móviles. Así doy paso al tema que se titula "**incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso"** manifestando que es importante que los niños, jóvenes y adolescentes y a su vez la sociedad ecuatoriana conozca estas nuevas actividades delictivas en el ciberespacio para el estudio del concepto, cuáles son las personas afectadas, quienes son las personas que lo hacen y quiénes son sus víctimas y por ende la funcionabilidad de este nuevo derecho penal y cuáles son sus principales dificultades. Con la finalidad de resolver el problema del desconocimiento en la población y a su vez dar una dirección para su correcta tipificación a un futuro.

Analógicamente se han verificado los objetivos del presente trabajo de investigación curricular en el aspecto general que es "Realizar un estudio doctrinario respecto a la figura del ciberstalking" y del mismo modo los objetivos específicos que se encargan el primero de "Demostrar la existencia de la figura de ciberstalking en nuestra realidad y la impunidad de los delincuentes informáticos." Segundo "Realizar un estudio de derecho comparado en relación al delito de ciberstalking" Tercero "Proponer una propuesta de reforma al Código Orgánico Integral Penal respecto de la figura del ciberstalking."

Este trabajo investigativo fue fundamentado y estructurado con base a los antecedentes del ciberstalking, lo que comprende su actividad física denominada en normativa americana como stalking, su nuevo tipo de funcionabilidad en el ciberespacio y por ende los nuevos problemas en el derecho penal, y el estudio de esta nueva figura delictiva para un correcto estudio y su correcto análisis y su importancia de implementación en el Código Orgánico Integral Penal como punto clave para la estructuración de este proyecto. Todo lo anteriormente mencionado tiene un enlace directo con el derecho comparado de legislaciones como España, Estados Unidos y Reino Unido con la finalidad de comprender de manera subjetiva la normativa vigente en otros países para el uso en nuestra realidad nacional.

Conforman el proyecto de integración curricular, los materiales y métodos utilizados que tuvieron su función en la obtención de información relevante para sustentar la

investigación, además de las técnicas de encuestas y entrevistas realizadas, el estudio de casos Contribuyeron con la información optima, argumentada, precisa y concreta para fundamentar el presente trabajo de integración curricular, de igual modo, se ha logrado verificar el objetivo general de la investigación en conformidad con los tres objetivos específicos, que demuestran la necesidad de la implementación en nuestra legislación la figura del ciberstalking los mismos que fueron fundamentales en la fundamentación de la propuesta de reforma legal.

Para finalizar se exponen recomendaciones y conclusiones de este trabajo los mismos que sirven como fundamento para justificar el estudio de esta nueva figura a su vez que se analizan las casusas y soluciones que se han llegado al finalizar esta investigación,

De esta manera queda presentado este trabajo de investigación que trata sobre la necesidad de incluir la figura del ciberstalking como delito en el código orgánico integral penal y su persecución como forma de acoso, esperando que la investigación sirva como guía a los estudiantes y profesionales del derecho como fuente de consulta y conocimiento, quedando ante el tribunal de grado para su corrección y aprobación.

4. Marco Teórico

4.1. Derecho penal

El derecho penal ha evolucionado a lo largo de la historia, el mismo ha sido influenciado por diferentes factores, ya sea por las diferencias de creencias y valores de la época, las relaciones sociales, políticas y económicas, y los sistemas de gobierno.

En la antigüedad, el derecho penal se basaba en leyes escritas y en el uso de la fuerza para hacer cumplir las leyes y con ello el castigo a los delincuentes, los mismos eran a menudo crueles y desproporcionados.

Con el tiempo, el derecho penal ha sido participe del constante cambio, y con ello a la adaptación de la realidad social de la época, esto con el fin de hacer un enfoque más racional y humanitario. Por ejemplo, en la conocida Edad Media los derechos actualmente conocidos como los principios de inocencia presunción de inocencia comenzaban a surgir y asentar sus bases, los mismos que en la actualidad se encuentran en la mayoría de códigos penales como lo es la ecuatoriana que lo estipula en el COIP en su Artículo 5 en el numeral 4 en el mismo que establece que "toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal, mientras no se ejecutoríe una sentencia que determine lo contrario". Por otra parte, en el siglo XVIII y XIX, en Europa se da una transformación social y política basada en un contexto social el mismo que da paso a diferentes escuelas y por ende posturas filosóficas como lo es el iluminismo y el liberalismo los mismos que dan paso a un derecho penal mucho más "humanitario".

En la actualidad, el derecho penal sigue en constante cambio y a su vez se ha convertido en un sistema cada vez más complejo y actualizado. En el mundo existen diferentes sistemas de derecho penal, los mismos que cuentan con sus propias leyes y normas. Sin embargo, la mayoría de dichos sistemas comparten algunos principios fundamentales, como lo son la protección de los derechos humanos y la presunción de inocencia.

Con el surgimiento de estas nuevas sociedades la misma ha dado paso a unas penas y castigos más "humanizados" el Estado haciendo uso del derecho penal subjetivo ha dado paso a lo se conoce como el "Ius puniendi" que es una facultad netamente del Estado ya que es este y la entidad encargada que tienen las facultades para conocer y sancionar un delito y esto esencialmente es de lo que trata el derecho penal que el mismo lo podríamos definir como un conjunto de normas que rigen el comportamiento social del ser humano para vivir en armonía,

y al momento que este sea violentada sea impuesto un castigo y esta a su vez sea restituido el daño en lo máximo posible.

> La misión del derecho penal es la de todo derecho (porque el derecho penal sólo es un sector del derecho en su totalidad), a saber, la regulación de la convivencia humana. La convivencia social requiere preceptos jurídicos y un orden en que el individuo pueda vivir sin ser lesionado por otros (BAUMANN, 1973, pág. 7)

Entonces el derecho penal surge a partir de un contrato social que busca la convivencia pacífica de un grupo de personas, con esto nace la idea de esta rama del derecho que usando normas legales con la finalidad de tener una forma de castigo hacia los infractores para que los individuos que conviven dentro de una misma comunidad puedes ser capaces en el caso de una lesión a sus derechos puedan recurrir al derecho penal para su protección o restitución en su máxima forma.

El derecho penal es "…El conjunto de normas jurídicas de carácter público que prohíben la comisión de un delito asociando a éste, como presupuesto, la pena y/o la medida de seguridad como consecuencia jurídica…" (Garcia, 2015, pág. 3)

Referente a lo anterior citado, con el avance de la sociedad, la forma punitiva que es potestad de un Estado avanza y por ende debe tener garantías para ambas partes, con esto se a hecho el derecho penal que es un conjunto de normas jurídicas que tienen la finalidad de ejecutar penas como finalidad de una acción negativa o prohibidas que afecten a la convivencia pacífica de una comunidad.

> El derecho penal es el conjunto de normas jurídicas que definen determinadas conductas como delito o como faltas y disponen la imposición de penas o medidas de seguridad. Es usado en todo proceso de criminalización y como forma de control social, y constituye el medio más enérgico del que dispone el Estado para evitar las conductas que resultan más indeseadas e insoportables para la sociedad (VILLVICENCIO, 2017, pág. 23)

El derecho penal en si es un sistema sancionatorio que arremete contra el presunto infractor, bajo este concepto, el Estado como ente sancionador y de control tiene la facultad de imponer penas de acuerdo al delito cometido, en si el derecho penal es la manera en que el estado mantiene en control a la sociedad por el medio de si un ciudadano con los resultados de sus actos a concatenar un resultado lesivo el mismo que en dicho país sea participe de una pena.

> derecho penal es un conjunto de normas y disposiciones jurídicas que regulan el ejercicio del poder sancionador y preventivo del Estado, estableciendo el concepto del delito como presupuesto de la acción estatal, así como la responsabilidad del sujeto activo y asociando a la infracción de la norma una pena finalista o una medida aseguradora (AZUA, 1990 citado en Cruz, 2017, pág. 3)

El derecho penal cuenta con dos relaciones, la primera que parte del estado como sujeto sancionador y el segundo que es el sujeto de protección, entonces el derecho penal al ser un conjunto de normas que sirven para regular estas penas para asegurar un debido proceso a los infractores y a su vez establecer las penas y el delito que en si se ha cometido y está tipificado.

4.1.1. Derecho penal o legislación penal

Referente a esto Zaffaronni nos dice que "El uso de la expresión derecho penal es equívoco: con frecuencia se la emplea para designar una parte del objeto del saber del derecho penal, que es la ley penal. La imprecisión no es inocua, porque confunde derecho penal (discurso de los juristas) con legislación penal (acto del poder político) y, por ende, derecho penal con poder punitivo, que son conceptos que es menester separar nítidamente, como paso previo al trazado de un adecuado horizonte de proyección del primero" (ZAFFARONI, 2000, pág. 4)

Con lo anteriormente referido se me hace necesario diferenciar estos dos conceptos que si bien no son lejanos guardan una diferencia importante para el avance de este proyecto de investigación por lo cual decimos que:

> **Derecho penal:** el derecho penal interpreta las leyes penales siempre en el marco de las otras leyes que las condicionan y limitan (constitucionales, internacionales, etc.) (ZAFFARONI, 2000, pág. 5)

> **Legislación penal:** es el material básico de interpretación del derecho penal. En primera aproximación, puede entenderse por legislación penal al conjunto de leyes que programan la decisión de conflictos mediante una coerción que priva de derechos o infiere un dolor (pena) sin perseguir un fin reparador ni de neutralización de un daño en curso o de un peligro inminente. (ZAFFARONI, 2000, pág. 37)

D0ecimos entonces que la diferencia entre estos dos conceptos es que la legislación penal son las leyes en sí, y el derecho penal es el encargado de la interpretación de las mismas.

4.1.2. Derecho penal del enemigo

El derecho penal del enemigo es un concepto bastante discutible, el mismo se refiere a una perspectiva del derecho penal en el cual su teoría parte conceptualizando a algunos delitos y delincuentes de una manera no igual (diferenciada) y a la vez más severa que a otros, esto en función a que esta persona pertenezca a un grupo considerado como un "enemigo" de una sociedad o directamente del Estado. Este enfoque ha sido utilizado en algunos regímenes autoritarios y totalitarios, con el fin de justificar la represión y la discriminación contra disidencias políticas, minorías étnicas o culturales, o grupos sociales percibidos como "amenazantes" o como el “enemigo” para la estabilidad o seguridad del régimen. Desde un punto de vista ético-jurídico, el derecho penal del enemigo se puede considerar como inaceptable porque viola los derechos humanos y algunos principios como lo es el de igualdad ante la ley.

Para Martínez el derecho penal del enemigo se sustenta en tres ejes fundamentales los cuales son:

1.- Adelanta la punición de determinadas conductas aun antes de que se consuma la ejecución de las mismas: El primer eje a tratar nos habla de la "prevención penal". La prevención penal es una técnica utilizada en el derecho penal la misma que consiste en adelantar la punición o sanción por un delito o conducta delictiva, aún antes de que se haya consumado su ejecución. Esto con el objetivo de prevenir la comisión de delitos y proteger la seguridad en la sociedad. Algunos ejemplos de medidas de prevención penal son: el arresto preventivo, la confiscación de bienes relacionados con el delito y el control de la residencia. Sin embargo, la aplicación de la prevención penal sel debe hacerse de manera proporcionada y respetando los derechos humanos, ya que puede dar lugar a abusos y a la privación ilegítima de libertad.

2.- Castiga determinadas conductas que no se han hecho con la misma penalidad que si se hubiese realizado: El segundo eje a tratar se trata de la "teoría del delito". En el derecho penal, la teoría del delito es la que establece las condiciones y requisitos necesarios para que una conducta sea considerada delictiva y, por lo tanto, merecedora de sanción o pena. Esta teoría se basa en la idea de que la conducta humana debe ser castigada sólo cuando cumple con determinados requisitos, como la intencionalidad, la antijuricidad y la culpabilidad. La idea es que una conducta no puede ser castigada si no se ha realizado de manera voluntaria y consciente y si no ha causado daño a terceros. De esta forma, se busca garantizar la igualdad ante la ley y la protección de los derechos humanos, pero si bien, aunque lo anteriormente dicho

y de acuerdo a esta característica del derecho del “enemigo” también tiene el mismo grado de pena, aunque no se hubiera realizado o llegado a concretar la actividad que tiene como finalidad causar daño o afectar al patrimonio ajeno.

3.- Se establece una serie de medidas que reducen garantías individuales: El tercer eje trata de las “medidas excepcionales o restrictivas". Las medidas excepcionales o restrictivas son aquellas que se establecen en situaciones de emergencia o crisis, como conflictos armados, disturbios sociales o pandemias, para proteger la seguridad y el orden público, o a su vez bajo el contexto del derecho penal del enemigo se refiera al resguardo y pronta exclusión del “enemigo” con el fin de precautelar y prevenir un posible delito. Estas medidas pueden incluir la restricción de la libertad de movimiento, la limitación de la libertad de expresión, la confiscación de bienes y la intercepción de comunicaciones. Sin embargo, estas medidas también pueden tener un impacto negativo en las garantías individuales y los derechos humanos, ya que reducen la libertad y la privacidad de las personas. Por lo tanto, es importante que se implementen de manera proporcionada, limitada en el tiempo y con un control judicial adecuado para evitar abusos y garantizar la protección de los derechos humanos.

Si bien explicado hasta este punto el derecho penal el “enemigo” se me hace menester plantear en este proyecto de investigación una diferencia entre el derecho penal del enemigo y del ciudadano ya que más adelante explicare una nueva realidad del derecho penal en el mundo virtual para lo cual es imprescindible saber la diferencia y conocerlos para su explicación, entonces para dar esta diferencia me valdré del siguiente concepto:

> “El Derecho Penal del Enemigo y del Ciudadano son dos conceptos dogmáticos desarrollados principalmente por el catedrático de la Universidad de Bonn Gunther Jakobs, quien ha manifestado que el Derecho Penal posee dos perspectivas de las personas al momento de intervenir con la aplicación del Ius Puniendi, una orientada hacia las personas que infringen la norma y por ende merecen una pena denominados “ciudadanos”, y otra para aquellas personas que contravienen el ordenamiento jurídico de tal forma que son considerados enemigos.” (ROMERO, 2021, págs. 549-550)

Digo que el derecho penal del ciudadano es un enfoque del derecho penal que se centra en la protección de los derechos individuales y libertades de los ciudadanos. Este enfoque se basa en la idea de que la función principal del derecho penal es proteger los derechos y las libertades individuales y limitar la intervención del estado en la vida de las personas. En lugar de ser utilizado como un instrumento de represión gubernamental, el derecho penal del

ciudadano se utiliza para proteger a los individuos de la injusticia y para garantizar que los castigos se apliquen de manera justa y proporcionada. Este enfoque se opone a la idea del derecho penal del enemigo, que defiende la idea de que los derechos individuales.

Y por su contraparte el derecho penal del enemigo se encarga de regular las relaciones entre el estado y aquellos que son considerados "enemigos" de la sociedad, ya sea en tiempos de paz o de guerra. Según esta teoría, en situaciones de emergencia nacional, el estado tiene el derecho a limitar los derechos humanos y las libertades individuales de los enemigos de la sociedad, ya sea por motivos de seguridad o para proteger el bienestar de la sociedad en general. Esta teoría ha sido criticada por justificar la limitación de derechos humanos en situaciones de crisis y por su carácter autoritario.

El concepto del derecho penal del enemigo fue propuesto por el jurista alemán Günther Jakobs y el mismo se refiere a una nueva forma de aplicación el Derecho penal, en el cual se aplica una separación y a su vez un concepto diferenciado entre dos tipos de personas las cuales a las primeras las denomina como "ciudadanos" y por su contraparte aquellos denominados como "enemigos"

Se argumenta que las personas que viven en una sociedad y son vistos como "enemigos" o "amenaza" no son susceptibles a un mismo trato, es decir, la protección de sus derechos y garantías no son iguales a las personas que son consideradas como "ciudadanos". Con esto decimos que, esta teoría versa en que se debe tener un trato más severo a aquellas personas que son considerados "enemigos" incluso en un contexto social donde prevalezca la paz, para entender mejor esta teoría algunos puntos clave o características son:

1. **Diferenciación de categorías:** Como se señaló anteriormente la diferenciación es esencial en esta teoría, dando así dos clases, en la primera los "ciudadanos" que tienen su característica en que reciben protección en sus derechos y a su vez el derecho a un debido proceso, y por su contraparte, los "enemigos" de una sociedad los mismos que son tratados con más dureza y esto es reflejado en una limitación o restricción en sus derechos.
2. **Limitación de derechos fundamentales:** Esta característica solo es una atribución a los ya denominados "enemigos", el Estado ya sea por situaciones de emergencia, o situaciones que tengan con objetivo precautelar el bienestar de la sociedad, este tiene el derecho en limitar tanto libertades individuales y derechos humanos.

3. **Enfoque preventivo:** Esta teoría no se basa en el enfoque de protección de derechos y una adecuada rehabilitación del delincuente o como se lo denomina un "enemigo", esta teoría se enfoca más en la prevención y una correcta anulación de amenazas potenciales.

Sin embargo, esta teoría tiene algunas críticas entre las cuales las más destacadas son:

1. **Erosión de garantías legales:** Esta teoría abre las puertas a abusos de poder, ya que la práctica del derecho penal del enemigo lleva a una erosión en los derechos fundamentales los mismos que sirven para la protección de los individuos.
2. **Discriminación y estigmatización:** La misma comienza en la propia conceptualización de la teoría, desde el momento en que se usa una diferenciación con los conceptos de "ciudadano" y "enemigo" da paso a este problema de discriminación lo cual lleva a un problema de "choque de clases" en una sociedad.
3. **Riesgo de abuso de poder:** Este riesgo se da por el excesivo poder que tendría el estado en juzgar a la sociedad, lo que podría conducir a prácticas autoritarias y violaciones de derechos humanos.

Para concluir con la explicación de la teoría del derecho penal del enemigo, en el instante en que me refiero a un "carácter autoritario" hago referencia a que dicha teoría, en mi opinión, lleva a las características de un sistema autoritario, y me baso en que el poder que se le confiere al Estado es excesivo y no limitado hacia aquellos individuos de una población denominados como "enemigos".

4.1.3. Derecho penal sustantivo y adjetivo

Para el presente proyecto de investigación nos referiremos al derecho penal sustantivo, pero a su vez al hablar del sustantivo se me hace indispensable hablar de la interdisciplinariedad en el derecho penal procesal los cuales son dos tanto el derecho penal sustantivo y el adjetivo.

Entonces decimos que el **derecho penal sustantivo** son aquellos conjuntos de normas que hablan de los delitos y sus respectivas penas, medidas de seguridad. Esta tiene como objetivo que el Estado como ente que impone la "justicia" controle estas conductas penalmente imputables.

En otras palabras, el derecho penal sustantivo es aquella rama del derecho que se encarga de regular las relaciones entre individuos y entre éstos y el Estado, estableciendo normas y principios a los cuales deben ajustarse dichas relaciones. Este derecho tiene como objetivo principal proteger los derechos y libertades de las personas y regular la conducta humana en sociedad.

Entonces decimos que el **Derecho penal adjetivo** son aquellos conjuntos de normas que tienen el propósito de garantizar el cumplimiento de los derechos y obligaciones del derecho sustantivo

En otras palabras, el derecho penal adjetivo trata sobre la regulación de los delitos y las penas correspondientes. Se encarga de definir los comportamientos considerados delictivos, establecer las normas y las sanciones aplicables a los autores de los mismos, y garantizar la protección de los derechos y libertades de la sociedad y de los individuos.

En el derecho penal adjetivo se establecen las reglas para la persecución y el castigo de los delitos, con el objetivo de prevenir su comisión y proteger a la sociedad y a los individuos de los comportamientos considerados delictivos. Además, también se regulan las garantías y los derechos de los acusados y las víctimas, garantizando un debido proceso justo.

En resumen, el derecho penal adjetivo trata sobre la regulación de los delitos y las penas aplicables a los autores de los mismos, con el objetivo de proteger a la sociedad y a los individuos, y garantizar el respeto a los derechos y libertades fundamentales.

Para finalizar concluyo que, si bien son parecidos, por no iguales, el derecho penal sustantivo es la norma, la parte fija, inmóvil y el derecho penal adjetivo es la parte móvil, activa.

La constitucionalidad del derecho penal, es un complejo proceso social y jurídico en el cual se basa en una adhesión y aplicación de garantías fundamentales, principios y derechos consagrados en la Constitución en el ámbito penal de todo un Estado. La evolución, o más bien la adaptación constante en el ámbito punitivo se basas en un contexto social, ya que como sabemos el derecho se adapta de acuerdo a la realidad social en la que se vive, esto para dar una respuesta a una serie de experiencias históricas de violaciones a los derechos humanos y el abuso de poder, da la necesidad de establecer un nuevo sistema punitivo en el cual se respete la dignidad y libertades individuales, aunque este hasta la fecha se encuentra en un nuevo proceso de adaptación a los nuevos problemas de una sociedad que se encuentra en las puertas de una

nueva era, la era informática, este concepto, como lo dije anteriormente, se basa en procesos históricos como son:

1. **Surgimiento de los derechos humanos:** La idea de la protección de los derechos humanos ha sido un tema tratado desde hace ya muchos años, los mismos que en el siglo XVIII, durante las revoluciones liberales, se dan las bases para algunos derechos modernos tales como es el derecho a la libertad y a la igualdad.
2. **Revolución francesa y la Declaración de los Derechos del Hombre y del Ciudadano (1789):** Esta declaración estableció principios como la presunción de inocencia, el derecho a un juicio justo y la prohibición de la tortura, sentando las bases para la protección de los derechos fundamentales en el ámbito penal.
3. **Codificación del derecho penal:** En el siglo XIX, muchos países adoptaron códigos penales los cuales incorporaban principios fundamentales del derecho penal, como lo son: la legalidad, la proporcionalidad de las penas y la individualización de las sanciones.
4. **Internacionalización de los derechos humanos:** En el contexto histórico de que el mundo después de la Segunda Guerra Mundial, con la creación de las Naciones Unidas y la adopción de la Declaración Universal de Derechos Humanos (1948), los derechos humanos fundamentales fueron objetivos de preocupación mundial y por ende muchos países fueron parte de la misma, dando así la internacionalización de los derechos humanos.

Con las bases sociales e históricas de la constitucionalización del derecho penal podemos decir que sus principales características son:

Jerarquía constitucional: La constitución se basa en principios y garantías de carácter jerárquico superior a comparación a otras normas, las mismas que son incorporadas al derecho penal, entonces, esto tiene un significado en el cual los preceptos en el derecho penal deben estar en correlación con los preceptos constitucionales con la finalidad de declarar nula o inconstitucionalidad aquellas normas que transgredan los preceptos constitucionales.

Protección de los derechos fundamentales: La siguiente característica versa en el objetivo propio de la constitucionalización en el derecho penal, el mismo que trata y

tiene como objetivo principal la protección de derechos y principios fundamentales algunos como: presunción de inocencia, igualdad, libertad etc. Los mismos que en ningún momento podrán ser vulnerados.

Principio de legalidad: En el derecho penal el principio de legalidad se basa en que no existe un castigo para una acción que no esté tipificada o prevista en la ley penal que en nuestro caso sería el COIP. Lo que hace la constitucionalización es un refuerzo al mismo haciendo así que se exija a las leyes penales sean más claras y precisas.

Prohibición de penas crueles o inhumanas: Como se ha explicado antes, las sanciones en lo largo de la historia han sido de carácter desproporcionado e inhumano, ahora, la ayuda de la constitucionalización del derecho penal ayuda a prevenir dichas conductas, esto con el fin de asegurar que las sanciones impuestas sean proporcionales a la gravedad del delito cometido.

Limitación del poder punitivo estatal: Establecido en la constitución, el mismo establece límites claros al poder punitivo del Estado, garantizando así tanto su aplicación de manera proporcionada del derecho penal.

4.1.4. Derecho penal en el ciberespacio

Más que dar una nueva forma del derecho penal dentro del concepto o marco de la virtualidad, solo volveremos a pensar o repensaremos cómo funciona el derecho penal en relación a las conductas que se realizan dentro del ciberespacio.

Bien, para empezar la idea de la funcionalidad del derecho penal en un mundo virtual, suena difícil o algo complicado, pero, la realidad es todo lo contrario, el derecho penal en el ciberespacio funciona de la misma forma de la criminalidad del mundo real, entonces bajo esta aseveración, si funciona igual ¿Por qué es un tema importante a tratar? ¿Por qué en la actualidad es tan difícil hacerle frente a un delincuente informático?

Las preguntas antes planteadas las tratare de abarcar con el fin de explicar por qué de la impunidad que tiene el delincuente en la legislación ecuatoriana e internacional y ya que este es un problema de la era digital tratare de dar una solución a la misma, y a su vez veremos porque la solución es una limitación de derechos como es la libertad y intimidad, lo cual en países en vías de desarrollo el control digital es una idea utópica.

Abarcando el primer punto **¿Por qué es un tema importante a tratar?**

El análisis y por ende la importancia del estudio del derecho penal en el ciberespacio es fundamental por varias razones:

1.- Protección de los derechos humanos: El derecho penal en el ciberespacio es el encargado de proteger los derechos humanos en el entorno digital, esto incluye la privacidad, la libertad de expresión y la protección de datos personales, pero si bien este es una "nueva rama del derecho penal actual" para el "combate" o a su vez la palabra "protección" del ciberdelincuente ha sido una constante al derecho llamado intimidad, ya que cuando la libertad, intimidad y el anonimato y a su vez la modificación de datos personales impidiendo que la policía cibernética no pueda detectar al autor se da una especie de indefensión de la persona que es afectada, a esto me gustaría llamarlo como el marco de superioridad del autor a la víctima.

Ya que abarcamos el problema de la privacidad, en la legislación ecuatoriana, según el artículo 66 de la Constitución de la Republica del Ecuador, en el capítulo sexto, de los derechos de libertad en su numeral 20 estipula: "El derecho a la intimidad personal y familiar". (Consitución de la Republica del Ecuador, 2008, pág. 27) Por ende, en dicho articulo manifiesta que el derecho de la intimidad es un derecho fundamental de la libertad personal y por ende un problema actual para la correcta intervencion, pero ¿esto ya se a hecho en alguna otra parte o se a planteado? La respuesta es si y me basare en una norma complementaria peruana como lo es la ley 27.697 la misma que le da la facultad al fiscal a intervenir y controlar comunicaciónes y documentos privados en supuestos excepcionales, si bien, la misma que faculta al fiscal en intervenir en casos establecidos en casos como secuestro agravado, trafico de menores, robo agrabado, extorcion agrabada, trafico ilisito de drogas, asociasion ilicita para delinquir, deñitos contra la humanidad, pornografia infantil, etc esto seria una forma directa de ataque al derecho a la privacidad pero a su vez con una justificacion para el resguardo del derecho de otra persona frente a una conducta delictiva como lo es el acoso cibernetico y por ende el tipo penal estudiado como es el ciberstalking.

Para concluir, para el correcto castigo o detección del ciberdelincuente se podría dar la facultad al fiscal o a la policía cibernética la facultad de la intervención de datos o si bien el control de que la población en el uso del internet o en dispositivos, entonces el derecho a la privacidad será limitado en este aspecto y los datos recolectados por entidades competentes no podrán ser difundidos a menos que se lo requiera y con ello se daría un paso importante para el control del ciberespacio y por ende la facilidad en la captura de los ciberdelincuentes.

2.- Regulación de la conducta en línea: El derecho penal cibernético regula la conducta en línea y establece sanciones para aquellos que cometan delitos en el entorno digital, como la ciberdelincuencia, la ciber violencia y la suplantación de identidad.

Entonces lo decimos muy fácil, pero para referirme a una correcta regularización, en el ámbito de la importancia del estudio y castigo del ciberdelincuente no es un problema nacional, es un problema internacional y en parte los problemas de perseguibilidad en el ciberespacio, y con esto citare lo que nos dice Riquert:

> Los matices de grado y forma con que se consolida en cada país o región aquel impulso político-criminal internacional (Cooperación, asimilación, armonización o unificación normativa), naturalmente, vienen condicionados por una serie de filtros valorativos propios en los que intervienen factores de distinta naturaleza (ideológicos, políticos, económicos y culturales). En última instancia, no hacen más que exteriorizar las dificultades en al canzar consensos ante la convergencia de intereses disimiles, aunque no necesariamente contrapuestos en forma absoluta. (RIQUERT, 2018, pág. 22)

Con lo anteriormente citado decimos que, si bien la regularización no solo es un problema nacional, ya que partiendo desde la premisa que el derecho penal cibernético es un problema mundial por lo que la red conecta a diferentes partes del mundo al mismo tiempo y a su vez cada país cuenta con su soberanía, por lo cual su correcta sanción y persecución se ha convertido en una odisea y su castigo una utopía. Para partir con la explicación quisiera decir que lo he dividido de acuerdo a la dificultad de implementar un acuerdo internacional o para evitar paraísos de impunidad. En el contexto de la consolidación del impulso político-criminal internacional, los factores de valoración en la que se desarrolla en cada país o región están influenciados por diferentes circunstancias. Los factores, antes mencionados, incluyen consideraciones tanto culturales, ideológicas, políticas e ideológicas las mismas que son claves para poder determinar las tres fases que son la cooperación, asimilación, armonización o unificación normativa. La dificultas que presentan alcanzar la aprobación absoluta se basa en la convergencia de intereses disimiles, sin embargo, los intereses divergentes no son necesariamente opuestos. Aunque en la actualidad hay la existencia muy diversa tanto en perspectivas y enfoques para la aplicabilidad en el tema de la aplicación en el tema de las políticas criminales a nivel internacional el mismo que da paso a muchas opciones para una correcta consolidación en dichos impulsos.

La cooperación entre países y regiones es el primer enfoque en el que hay que adaptarse. Con esto quiero decir que implica el trabajo conjunto entre naciones este con el fin de abordar problemas y desafíos comunes en el ámbito de la justicia penal internacional. La cooperación puede manifestarse a través de acuerdos bilaterales o multilaterales, intercambio de información, asistencia mutua en investigaciones y enjuiciamientos, entre otras formas de colaboración.

La asimilación entre los países y regiones es el segundo enfoque es en el que hay que guiarse con el fin de la adopción de normas y políticas criminales similares a las de otros actores internacionales, con la finalidad de que se haga una adaptación a las diferentes realidades sociales. Este enfoque se basa en la implementación de estándares y prácticas internacionales en un ámbito político-criminal con el objetivo de la búsqueda de una mayor coherencia y alineación de sus principios compartidos.

La armonización normativa comprende el tercer enfoque el cual los diferentes países o regiones en la búsqueda de consensos para una regulación penal. En este enfoque, la característica principal se basa en determinar un marco legal para la polémica contra el crimen transnacional el mismo que permita a su vez una mejor cooperación y coordinación.

_Nivel uno (Fácil), Cooperación: La fase de cooperación, lo he puesto en el estaño más inferior y por ende más fácil de conseguir, ya que las fronteras nacionales solo han ocasionado un obstáculo en la lucha de la perseguibilidad del ciberdelincuente y por ende su castigo ya que este usa las TIC como “un lugar sin fronteras” es por esto que los mismos países reconocen a la cooperación como algo que no se puede evitar y por ende y en su mayoría de casos se da de una manera muy rápida

Entonces concluimos que la armonización es el proceso de creación de normas y leyes penales similares en diferentes países o regiones del mundo, con el objetivo de asegurar una protección adecuada de los derechos humanos y una aplicación uniforme de la justicia penal. Esto se logra a través de la cooperación internacional y el intercambio de información y buenas prácticas entre los Estados. La armonización internacional del derecho penal también puede incluir la adopción de tratados internacionales, el mismo que es un punto a abordar en el nivel tres, y acuerdos multilaterales sobre temas específicos como la lucha contra la corrupción, el terrorismo, el tráfico de drogas y también los ciberdelitos como lo es la figura del ciberstalking

_Nivel dos (Medio), Asimilación y armonización: Para comenzar con la explicación comenzare citando a Riquert que nos dice

> La primacía de la técnica de la “armonización” se ha decido, fundamentalmente, a los inconvenientes de orden político y práctico para avanzar con la técnica de la “asimilación”. Esta última supone que la defensa de los intereses comunitarios se acomete mediante la remisión a la norma penal nacional que tiene como objeto la tutela de intereses nacionales semejantes (Se habla de “estrategia de descentralización mediante reenvió”) lo que implica la renuncia a la creación por parte de las comunidades de un derecho penal propio, ofreciendo el inconveniente de la desigualdad, ya que la defensa de los intereses nacionales propios no es idéntica en los distintos países (conductas punibles en unos pueden no serlo en otros), ni es equivalente la pena que a las mismas conductas que se imponen. La armonización, en cambio, se concreta sobre todo a partir de directivas comunitarias que ordenan la creación de nuevas normas de derecho interno con criterio compartidos que aseguren la igualdad necesaria para el funcionamiento mismo de las comunidades. No se trata de la imposición de una cultura o axiológica entre países, sino de algo más modesto, intentar la creación de condiciones uniformes (RIQUERT, 2018, pág. 30)

Con lo anteriormente dicho la técnica de "armonización" en lugar de la técnica de "asimilación" en la defensa de los intereses comunitarios. La asimilación se basa en remitir a la norma penal nacional y renunciar a la creación de un derecho penal propio, lo que conduce a la desigualdad. Por el contrario, la armonización se concreta a través de directivas comunitarias que ordenan la creación de nuevas normas internas con criterios compartidos para asegurar la igualdad necesaria para el funcionamiento de las comunidades. La armonización no implica la imposición de una cultura o valores entre países, sino intentar crear condiciones uniformes.

Entonces lo más correcto sería la armonización entonces me basare en lo dicho por Nieto Martin “el proceso de armonización como tal es pasible de críticas que pueden sistematizarse como procedentes de cuatro diferentes direcciones: 1) la relativa a su "extensión", en cuanto este proceso estaría propiciando una expansión del derecho penal dudosamente compatible con el principio de ultima ratio; 2) la concerniente a su "legitimidad", en cuanto contribuiría a erosionar el principio de legalidad; 3) la referida a la "intensidad", ya que la armonización debiera ceñirse en su pretensión de tipificaciones y sanciones a lo mínimo imprescindible, dejando un amplio espacio de juego al legislador nacional; 4) la relativa a la "calidad", en virtud de que bajo una premisa armonizante se minaría la calidad del derecho penal nacional por el uso de conceptos excesivamente vagos y penas desproporcionadas que romperían la armonía de los códigos penales nacionales.” (MARTIN, 2010, pág. 229)

Lo cual, si bien es una alternativa, no es la más segura ya que tiene sus desventajas, así como lo señala Martin, dado que en países de Latinoamérica (en su gran mayoría incluida la ecuatoriana) las previsiones procesales han sido diseñadas en base a la evidencia física y no tanto la digital, lo que puede generar dificultades en la presentación y valoración de la evidencia digital en los procesos judiciales. Esto significa que las reglas procesales no están específicamente diseñadas para tratar la evidencia digital, lo que puede resultar en soluciones improvisadas y la aplicación de criterios y reglas de las pruebas físicas de manera analógica.

_Nivel tres (Difícil), Unificación normativa: Ahora bien, la cima y por ende más difícil de alcanzar para una solución o ayuda en la "lucha contra la ciberdelincuencia" sería una unificación normativa.

La unificación normativa se refiere a la creación de un conjunto uniforme de reglas y normas para regular ciertas actividades. Esto puede implicar la armonización de leyes existentes o la creación de nuevas normas para lograr un alto grado de coherencia y comparabilidad en un área específica. La unificación normativa puede tener como objetivo mejorar la eficiencia, aumentar la transparencia y fomentar la confianza en un sector determinado, así como facilitar el comercio transfronterizo, el flujo de información, cooperación internacional y a su vez que los delitos informáticos tengan un castigo y no se deje en la impunidad.

Un ejemplo de unificación normativa en delitos informáticos puede ser la Convención de Budapest sobre Ciberdelitos, adoptada en 2001 por el Consejo de Europa. La Convención de Budapest es un tratado internacional que establece un marco común para la persecución y prevención de delitos informáticos, tales como el hacking, la suplantación de identidad, la difamación en línea, etc. La Convención también establece normas para la cooperación entre los países y la cooperación entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios en línea.

La convención de Budapest ha sido ratificada por varios países de Europa, así como países fuera de Europa y han sido elogiada como un paso importante hacia la unificación normativa en el ámbito de los delitos informáticos a nivel internacional, a continuación, incluiré la tabla, de dicho convenio, de las conductas que cada estado que formo parte debió adoptar a su derecho penal sustantivo, a continuación, se expondrá los ciberdelitos en Ecuador tipificados en el COIP y los expuestos en el convenio de Budapest.

DELITOS CIBERNETICOS EN ECUADOR

COIP ACTULIZADOS AL 2023

Art. 103 Pornografía infantil	13-16 años	**Art. 173 Contacto con finalidad sexual con menores de 18 años por medios electrónicos**	1-3 años
Art.174 Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7-10 años	**Art.178 Violación a la intimidad**	1-3 años
Art. 182 calumnia	6 meses a 2 años	**Art.186 Estafa**	5-7 años
Art. 190 Aprobación fraudulenta por medios alternativos	1-3 años	**Art.191 Reprogramación o modificación de información de equipos terminales móviles**	1-3 años
Art. 192 Intercambio, comercialización o compra de información de equipos terminales móviles	1-3 años	**Art.211 Supresión, alternación o suposición de identidad o estado civil**	1-3 años
Art. 229 Revelación ilegal de bases de datos	1-3 años	**Art.230 Interceptación ilegal de datos**	3-5 años
Art. 231 Transferencia electrónica de activo patrimonial	3-5 años	**Art.232 ataque a la integridad de sistemas informáticos**	3-5 años

Art. 233 Delitos contra la información pública reservada legalmente	5-7 años	**Art.234 Acceso no consentido a un sistema informático, telemático o de comunicaciones**	3-5 años
Art. 347 Destrucción de registros	7-10 años	**Art.354 Espionaje**	7-10 años
Art. 366 Terrorismo	10-13 años	**Art.234 Acceso no consentido a un sistema informático, telemático o de comunicaciones**	3-5 años

Fuente: Código Orgánico Integral Penal.

Medidas a nivel nacional: Derecho penal sustantivo. Conductas a tipificar		
Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos	***Acceso ilícito*** (Art. 2)	Tipificación del acceso deliberado e ilegítimo a todo o parte de un sistema informático.
	Interceptación ilícita (Art. 3)	Tipificación de la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.
	Ataques a la integridad de los datos (Art. 4)	Tipificación de todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
	Ataques a la integridad del sistema (Art. 5)	Tipificación de la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
	Abuso de los dispositivos (Art. 6)	Tipificación de la comisión deliberada e ilegítima de actos: a) de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos señalados en las celdas anteriores; ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer los delitos señalados en la celdas anteriores. b) la posesión de algunos de los elementos contemplados en i) o ii) del apartado a) con intención de que sean utilizados para cometer cualquiera de los delitos previstos en las celdas anteriores.
Delitos informáticos	***Falsificación informática*** (Art. 7)	Tipificación de la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.
	Fraude informático (Art. 8)	Tipificación de los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.
Delitos relacionados con el contenido	***Delitos relacionados con la pornografía infantil*** (Art. 9)	Tipificación de la comisión deliberada e ilegítima de los siguientes actos: a) producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) oferta o puesta a disposición de pornografía infantil a través de un sistema informático; c) difusión o transmisión de pornografía infantil a través de un sistema informático; d) adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e) posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.[2]
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	***Delitos relacionados con infracciones de la propiedad intelectual y derechos afines*** (Art. 10)	Tipificación de las infracciones de la propiedad intelectual que defina su legislación, conforme obligaciones contraídas en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derechos de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
		Tipificación de las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artista Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

Fuente: BCN, 2011. Revisado, julio 2018

Fuente: Convenio de Budapest.

Si bien, en la legislación ecuatoriana algunas de estas conductas criminales realizadas en el ciberespacio ya se encuentran tipificadas dentro del código orgánico integral penal y por otra parte otros han sido muy delimitados en su incorporación, así como el delito que es parte de este proyecto como lo es el ciberstalking

3.-Prevención de la ciberdelincuencia: Al estudiar el derecho penal cibernético, se pueden identificar y prevenir nuevos tipos de delitos en el entorno digital, lo que ayuda a mantener la seguridad en línea, en Ecuador, aunque su primer anuncio de un una Estrategia Nacional de Ciberseguridad (ENC) se anunció en el año del 2017 como una propuesta al combate a la ciberdelincuencia, la verdad no fue hasta el año 2022 que se elaboró un plan para el combate el cual establece su primera Estrategia Nacional de Ciberseguridad (ENC) la misma que cuenta con apoyo internacional con el fin de proteger tanto el sector público y privado, dicha estrategia se basa en 5 ejes:

_ Gobernanza y coordinación nacional.

_ Resiliencia cibernética

_Lucha contra la ciberdelincuencia

_ Ciberdelincuencia nacional y ciber inteligencia.

_ Habilidades y capacidades de ciberseguridad.

_Cooperación internacional.

Comenzando y dando un paso gigante Ecuador se adhiere al convenio de Budapest, anteriormente señalado, el mismo que a mi opinión es una decisión acertada para la prevención de la ciberdelincuencia, pero pasando a otras prevenciones que a mi consideración se deberían hacer serían las siguientes como ya se han hecho en Perú en las siguientes leyes:

_Otorga al fiscal la facultad de intervenir y controlar comunicación y documentos privados en supuestos excepcionales. (Ley 27.697)

_Crea el Registro Nacional de Terminales de telefonía Celular y establece prohibiciones y sanciones penales a quienes alteren u comercialicen celulares de procedencia dudosa (Ley 28.774)

_Establecer la vigilancia electrónica personal (ley 29.499)

_Sobre combate de la inseguridad ciudadana (Ley 30.076)

Dicho esto, aunque Ecuador apenas realizo su primera Estrategia Nacional de Ciberseguridad (ENC) y su reciente adición al convenio de Budapest, aún está empezando en los problemas de esta nueva era digital, y refiriéndome a las leyes peruanas que actualmente son unas de las legislaciones casi completas en Latinoamérica lo tomo de referencia y así espero que se tome de referencia igual para nuestra lucha con la ciberdelincuencia.

Para finalizar cuales son algunos temas a tener en cuenta para una correcta protección de una persona común para la prevención ante los delitos cibernéticos, Existen varias maneras de prevenir hacia la ciberdelincuencia, incluyendo:

Uso de software de seguridad: Instalar y mantener actualizado software de seguridad en todos los dispositivos, incluyendo antivirus, firewall y software anti-spyware, puede ayudar a proteger contra los ataques cibernéticos.

Contraseñas seguras: Utilizar contraseñas seguras y cambiarlas regularmente, así como habilitar la autenticación de dos pasos, los mismos pueden ayudar a proteger la información personal y financiera.

Educación y conciencia: Es importante tener conocimiento de las últimas amenazas cibernéticas y por ende tomar las medidas correspondientes para una correcta protección. En un ámbito más específico tanto las empresas y usuarios de forma individual deben recibir educación y formación sobre cómo mantener la seguridad en línea.

Verificación de correos electrónicos y descargas: Ser cuidadoso al momento de recibir y abrir correos electrónicos de correos desconocidos y por ende descargar archivos enviados en el mismo esto con el fin del evitar la propagación de los malwares.

Copias de seguridad regulares: Realizar copias de seguridad regulares de los datos y almacenarlos en un lugar seguro como puede ser en la nube o en su contraparte en un disco de almacenamiento externo.

4.-Adaptación a la tecnología en constante evolución: La tecnología sigue evolucionando rápidamente, y el derecho penal cibernético es importante para mantenerse al día con estos cambios y garantizar que la ley sea aplicable a la conducta en línea.

Este nuevo derecho penal en el ciberespacio se adapta a las nuevas realidades a través de la actualización constante de las leyes y regulaciones en relación a los delitos cometidos en el ciberespacio. Esto incluye la incorporación de nuevas tecnologías y formas de delincuencia en línea, así como la revisión y actualización de las penas y sanciones existentes. Además, la

cooperación internacional y la coordinación entre los diferentes países también son esenciales para garantizar la efectividad del derecho penal cibernético en el mundo digital globalizado de hoy.

En resumen, el estudio del derecho penal en el mundo digital o en el ciberespacio es fundamental para garantizar la seguridad y protección de derechos en un entorno digital.

Con lo anteriormente dicho, nos queda la interrogante **¿Por qué en la actualidad es tan difícil hacerle frente a un delincuente informático?**

Hay varias razones por las que es difícil hacerles frente a los delincuentes informáticos en la actualidad, las mismas que han sido abordas a fondo en la pregunta anterior

Anonimato: Muchos delitos informáticos se cometen desde países diferentes a los de la víctima o la jurisdicción en la que se lleva a cabo la investigación, lo que dificulta la identificación y localización de los delincuentes.

Tecnología avanzada: Los delincuentes informáticos tienen acceso a herramientas y tecnologías avanzadas que les permiten ocultar su identidad y su ubicación.

Cooperación internacional limitada: La falta de cooperación y coordinación entre las diferentes jurisdicciones y países también puede hacer que sea difícil hacerles frente a los delincuentes informáticos.

Derechos de privacidad: La protección de los derechos de privacidad y la protección de la información personal también pueden hacer que sea difícil obtener la información necesaria para investigar y perseguir a los delincuentes informáticos.

Si bien son temas ya tratados anteriormente, pero vale la pena su ratificación con el fin de decir el porqué de la dificultad, que este problema actual tiene y como muchos países es una tarea casi imposible.

4.2.Delito

El delito es un concepto que ha evolucionado a lo largo de la historia. En la antigüedad, el delito se consideraba una ofensa contra los dioses o contra el orden natural, y se castigaba mediante la expulsión o la pena de muerte. Con el tiempo, el concepto de delito comenzó a relacionarse con la ofensa a la ley humana y a los derechos de los demás.

En la Edad Media, el delito se entendía como una transgresión a las leyes divinas o a la ley natural, y se castigaba mediante la pena de muerte o la mutilación. En la modernidad, el

delito ha sido definido como un acto contrario a las leyes penales de un Estado, y se castiga mediante la prisión, la multa o ambas.

En la actualidad, el delito sigue siendo un concepto controvertido y sujeto a debate en diferentes sociedades. Algunas personas creen que el delito es una ofensa contra la sociedad y que debe ser castigado de manera severa, mientras que otras creen que el delito es el resultado de factores sociales, económicos o psicológicos, y que debe ser tratado de manera más compasiva.

Actualmente, el delito puede ser tratado de varias maneras, dependiendo de la naturaleza del delito y de la política criminal de cada país o región. Algunas opciones comunes para tratar el delito incluyen:

1. **Prisión:** La prisión es la pena más comúnmente asociada con el delito. Las personas que son condenadas por delitos graves pueden ser enviadas a prisión por un período de tiempo determinado.
2. **Multa:** Las multas son una forma común de castigo por delitos menores. Las multas son generalmente menos costosas que la prisión y se consideran una forma más compasiva de tratar el delito.
3. **Trabajo comunitario:** Algunos delincuentes pueden ser condenados a realizar trabajo comunitario como parte de su castigo. El trabajo comunitario puede incluir actividades como limpiar parques o ayudar en refugios para personas sin hogar.
4. **Rehabilitación:** La rehabilitación puede incluir terapias o programas de tratamiento diseñados para ayudar a las personas a entender y controlar sus comportamientos delictivos.
5. **Medidas alternativas:** Algunos delincuentes pueden ser condenados a medidas alternativas como la libertad condicional o la supervisión electrónica. Estas medidas permiten que las personas cumplan con su condena fuera de la prisión, siempre y cuando cumplan con ciertas condiciones.

Nos dicen que el "...delito es la conducta descrita por la ley penal cuya comisión supone la imposición de una pena o de una medida de seguridad; delito es lo que la Ley dice que es delito…" (Garcia, 2015, pág. 3)

El delito es una acción que es realizada por el ser humano el cual puede ser doloso o, esta tiene como consecuencia el daño hacia otra persona a su ve daño al patrimonio de la misma dando así una conducta que transgrede a la norma.

El delito es una conducta que es considerada ilegal y antijurídica por las leyes penales y cuya comisión conlleva a una sanción penal. La ley define qué acciones son consideradas delitos y establece las penas y medidas de seguridad correspondientes para cada caso. La ley es la que determina qué acciones son consideradas delitos y cuáles no lo son.

> El delito consiste en "…El acto humano realizado por diversas motivaciones y que violentan los derechos de las personas se le ha denominado delito…" (VALLEJO, 2010, pág. 9)

El delito es una acción que es realizada por el ser humano el cual puede ser doloso o, esta tiene como consecuencia el daño hacia otra persona a su ve daño al patrimonio de la misma dando así una conducta que transgrede a la norma.

El delito es un acto ilegal y antijurídico realizado por una persona, ya sea por motivos económicos, psicológicos o cualquier otra razón, que va en contra de los derechos de otras personas y sociedad en general. Estos actos son perseguidos y sancionados por las leyes y el sistema judicial.

> El delito es una conducta humana que se opone a lo que la ley manda o prohíbe bajo la amenaza de una pena. Es la ley la que establece que hechos son delitos, es la ley la que nomina que hecho va ser considerado como delito, es la ley la designa y fija caracteres delictuales a un hecho, si en algún momento esta ley es abrogada3 el delito desaparece. El delito es artificial. (MACHICADO, 2010, pág. 3)

Si bien, como aclaramos antes que el delito es una conducta humana que transgrede la norma, el derecho penal positivo es aquel que la ley es la única que puede decir cuales conductas son acreedoras a una sanción, pena y con esto llega lo que es la participación de la persona que al momento de transgredir o violar la norma es sancionada.

> El delito como acto típicamente antijuridico imputable y culpable, sometido a veces a condiciones objetivas de penalidad y que se halla conminado con una pena o, en ciertos casos, con determinada medida de seguridad en reemplazo de ella (VALLEJO, 2010, pág. 11)

La comisión de un delito es aquella conducta que el ser humano realiza con la finalidad de hacer daño a otra persona, por lo cual viola el pacto social lo cual, en la actualidad, son sancionadas con la finalidad de culpar y restaurar el daño lo máximo que se pueda.

4.3.Teoría del delito

La teoría del delito es una rama del derecho penal que se encarga de estudiar los elementos esenciales que deben concurrir para que un comportamiento humano sea considerado delictivo. La historia de la teoría del delito se remonta a la antigua Grecia, donde los filósofos discutieron sobre la naturaleza del delito y la justicia. Con el surgimiento del derecho romano, la teoría del delito adquirió un carácter más formal y se desarrollaron conceptos como el delito como acción prohibida y el castigo como sanción. Durante la Edad Media, el derecho canónico y el derecho feudal influenciaron en la teoría del delito. En la Ilustración, filósofos como Cesare Beccaria y Jeremy Bentham abogaron por un enfoque más racional y humanitario en la justicia penal. En la actualidad, la teoría del delito sigue evolucionando y adaptándose a los cambios sociales y tecnológicos como lo son los ciberdelitos.

> La teoría del delito tiene como objeto analizar y estudiar los presupuestos jurídicos de la punibilidad de un comportamiento humano sea a través de una acción o de una omisión, en estos términos dicho análisis no sólo alcanza a los “delitos” sino incluso a todo comportamiento humano del cual pueda derivar la posibilidad de aplicar una consecuencia jurídico penal, entonces, será objeto de análisis de la teoría del delito aquello de lo cual derive la aplicación de una pena o una medida de seguridad, así como los casos extremos en los que no obstante existir una lesión o puesta en peligro de un bien jurídico, el comportamiento humano resulte justificado, no reprochable, o bien, no punible. (VILLANUEVA, 2004, pág. 15)

La teoría del delito es un área del derecho penal que se ocupa de estudiar los presupuestos jurídicos que determinan la punibilidad de un comportamiento humano, ya sea mediante una acción o una omisión. Esta teoría analiza tanto los delitos como cualquier otro comportamiento que pueda dar lugar a una consecuencia jurídico-penal, incluyendo las situaciones en las que un comportamiento que lesiona o pone en peligro un bien jurídico resulta justificado, no censurable o no punible.

> La teoría del delito, como sistema de filtros que permiten abrir sucesivos interrogantes acerca de una respuesta habilitante de poder punitivo por parte de las agencias jurídicas, constituye la más importante concreción de la función del derecho penal en cuanto al

> poder punitivo (negativo o represivo) habilitado por las leyes penales manifiestas. Por ello, la elaboración dogmático-jurídica ha alcanzado en este punto su desarrollo más fino, quizá a veces sobredimensionado en relación al resto del derecho penal. (ZAFFARONI, 2000, pág. 374)

La teoría del delito es vista como un sistema de filtros que permiten hacer preguntas sucesivas sobre la habilitación del poder punitivo por parte de las autoridades jurídicas. Es considerada una de las concreciones más importantes de la función del derecho penal en cuanto a su poder punitivo o represivo, permitido por las leyes penales.

> El Derecho penal prohíbe y sanciona con penas aquellas conductas que hacen peligrar gravemente la subsistencia de la sociedad. Si no se prohibiera y sancionara el homicidio, si el robo o la violación fueran conductas indiferentes para una sociedad, esta sociedad tendría los días contados; y por tanto también sus miembros, los ciudadanos. Tras la realización de tales conductas, que llamamos «delitos», procede la imposición y cumplimiento de sanciones (las penas). Previamente sin embargo es preciso declarar la responsabilidad de quien los llevó a cabo, mediante la imputación de responsabilidad. Este es el significado de la teoría jurídica del delito. (SANCHEZ, 2015, pág. 63)

El derecho penal tiene como objetivo prohibir y castigar con penas aquellas conductas que ponen en peligro gravemente la supervivencia de la sociedad. Si cualquier acción humana realizada que afecte a otro derecho ajeno como es la vida, no fueran considerados como conductas graves por la sociedad no podría existir una convivencia. Después de que se cometan estos actos, conocidos como "delitos", es necesario imponer y hacer cumplir sanciones o penas. Antes de eso, es necesario determinar la responsabilidad de quien los cometió a través de la imputación de responsabilidad.

> La teoría del delito es una parte de la ciencia del Derecho Penal; comprende el estudio de los elementos positivos y negativos del delito, así como sus formas de manifestarse. Los elementos positivos del delito configuran la existencia de éste, mientras que los elementos negativos constituirán su inexistencia; las formas de manifestación, se refieren a la aparición del mismo. La teoría del delito "atiende al cumplimiento de un cometido esencialmente práctico, consistente en la facilitación de la averiguación de la presencia o ausencia del delito en cada caso concreto (BETANCOURT, 2015, pág. 3)

La teoría del delito es una disciplina dentro del derecho penal que se encarga de analizar los elementos que componen un delito y cómo éstos pueden manifestarse. En otras palabras,

estudia los aspectos positivos y negativos que definen la existencia o inexistencia de un delito. La finalidad principal de la teoría del delito es ayudar a determinar si existe o no un delito en un caso particular.

4.4.Delitos informáticos

Para partir con la definición de que son los delitos informáticos se me hace de suma importancia partir desde el origen mismo de la era de la digitalización, o la revolución digital que se está viviendo en la actualidad.

Es difícil determinar una fecha específica para el comienzo de la revolución digital, ya que ha sido un proceso continuo que ha tenido lugar a lo largo de varias décadas. Sin embargo, algunos marcos de tiempo comunes que se mencionan para el comienzo de la revolución digital incluyen:

- **1950-1960:** Aquí se dan los primeros ordenadores personales comenzaron a aparecer en esta década, lo cual marcó el inicio de la revolución digital para ciertas personas.
- **1969:** Se da la creación del Protocolo de Internet (TCP/IP) en 1969 fue un hito importante para el desarrollo de internet y es considerado por algunos como el comienzo de la revolución digital.
- **1989**: La creación de la World Wide Web (WWW) en 1989 fue otro hito histórico importante para el desarrollo de la tecnología de la información y la comunicación y se considera por algunos como el inicio de la revolución digital.
- **1991:** La popularización que ha tenido internet y la creación de la WWW en la década de 1990 también es considerado por algunos como el inicio de la revolución digital.

Con esto decimos que la historia de la revolución digital se dio desde la mitad del Siglo XIX, con la invención del primer computador hasta la actualidad, muy bien con esto en mente podemos comenzar diciendo que si bien, esta revolución ha traído varios beneficios como son la comunicación, diversión y trabajo también ha sido una base de nuevos actos dentro de este mundo virtual, que si bien al inicio se pensaría ¿Qué daño podría traer un problema en un mundo inexistente al real? Al paso del tiempo se ha dado importancia ya que los daños son significativos y con esto se da paso a lo que son los delitos informáticos.

Los delitos informáticos, también conocidos como ciberdelitos, son delitos cometidos utilizando tecnología de la información y la comunicación (TIC), como internet o dispositivos

móviles. Aunque los delitos informáticos existen desde que se crearon los primeros ordenadores, se han vuelto más comunes y más sofisticados a medida que la tecnología ha avanzado.

Uno de los primeros delitos informáticos conocidos fue el ataque a los sistemas de la Universidad de Massachusetts en 1983. En este ataque, un grupo de estudiantes utilizó un ordenador para acceder a sistemas confidenciales y alterar los archivos.

A medida que internet se volvió más popular a principios de la década de 1990, los delitos informáticos comenzaron a incluir actividades como el phishing, el spamming y el ciberacoso. También se desarrollaron nuevos tipos de delitos informáticos, como el hackeo de sitios web y la distribución de virus informáticos.

Vallejo nos dice acerca de la historia y el surgimiento "El termino delito informático se acuño a finales de los años noventa, a medida que internet se expandió por toda Norteamérica. Después de una reunión en Lyuón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por los problemas que migraron a Internet. El "Grupo de Lyón" utilizo el termino para describir, de forma muy imprecisa, todos los delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos" (TERRY, 2002 citado en VALLEJO, 2010, pág. 13)

Con el tiempo, los delitos informáticos han evolucionado para incluir una amplia variedad de actividades ilegales, como el robo de identidad, el ciberterrorismo y la exposición de datos confidenciales. Los delitos informáticos son una preocupación creciente en todo el mundo y muchos gobiernos han adoptado leyes y regulaciones para hacer frente a estos delitos.

El Dr Vicente Vallejo define al delito informático como "… el acto típico, antijuridico, imputable y culpable, sancionado por una pena y cometido mediante ordenadores y demás recursos electrónicos y cibernéticos…" (VALLEJO, 2010, pág. 15)

Como lo menciana vallejo los delitos informáticos comparten un medio en común, que son las Tecnologías de la información y comunicación (TIC) que las usan con el fin del cometimiento que transgreden la norma y por ende afecta el ambiente de tranquilidad preexistente la misma que es un acto que amerita una pena.

"…se define todo acto ilícito penal que ha sido llevado a cabo a través de medios informáticos y que está ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes…" (Panizo, 2009, pág. 5)

En primera hay que diferenciar que todo acto ilícito es todo aquel acto que están clasificados como algo ilícito que son necesariamente sujetos a una sanción, y la otra seria que son actos inmorales, pero al no ser una acción que estén dentro de esta clasificación no presentan ninguna sanción, entonces los delitos informáticos bajo este concepto son toda acción que usando medios electrónicos causen una violación a una norma ya preexistente y con esto un daño a bienes o la integridad de un individuo, entonces solo así son susceptibles a una sanción
.

La realización de una acción que, reuniendo las características que delimitan el concepto de delito. Se ha llevado a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (DAVARA, 2008 citado en VALLEJO, 2010, pág. 15)

Los delitos informáticos, es simplemente el delito que ya se conoce habitualmente pero que use como medio los medios electrónicos, o a su vez usando hardware como lo son los Rapsberry pi zero w o el USB killer que causa un daño al computador, este también mencionando los daños por software donde entran los nuevos delitos electrónicos que son el uso de programas o simplemente redes sociales al momento de averiguar o alterar información.

toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas (González, 2013, pág. 45)

Nos dice que, los delitos informáticos se basan en la acción de expresar la voluntad del sujeto activo hacia el sujeto pasivo, esto a sabiendas que se provocara un delito o un daño a la persona, pero aquí en el desarrollo de estos delitos la gran diferencia con los delitos habituales realizados en el mundo físico se basa en que cuya comisión se usa o intervienen como medio de una forma activa los dispositivos que de forma general y cotidiana se usan para actividades informáticas como lo es en las actividades de la comunicación , entonces con todo lo anterior estudiado señalamos que un delito informático se caracteriza por las siguientes características:

1. **Acceso no autorizado:** Esta característica se basa en la obtención a los accesos de los diferentes sistemas informáticos o dispositivos el mismo sin el consentimiento del propietario o responsable del sistema, esto sin confundir dispositivos informativos con dispositivos electrónicos, este con una finalidad ya sea de un acceso, modificación o substraer información personal.
2. **Daño o alteración de datos:** Se basa en una modificación o eliminación, la misma que es intencionada, de datos, programas o sistemas con la finalidad de perjudicar a la víctima.
3. **Espionaje y vigilancia ilegal:** Se basa del acceso no autorizado ya sea a comunicaciones privadas o sistemas informáticos con fines de espionaje o vigilancia, definiendo al espionaje como aquel acceso a un dispositivo ajeno con la finalidad de obtener información ajena.
4. **Extorción digital:** Se basa en el conjunto de amenazas, intimidación o chantajes los mismos que tienen bastantes finalidades como pueden ser la obtención de dinero o como lo es en el caso del tema en investigación la finalidad de causar miedo, hostigamiento y hacer pasar un mal momento a un cibernauta ya sea que al mismo sea alguien conocido o no.

4.4.1. Los nuevos problemas de perseguibilidad en los delitos informáticos

La perseguibilidad de un delincuente se refiere a la capacidad de una autoridad, como una policía o un fiscal, de investigar y enjuiciar a una persona por un delito. Esta práctica ha existido durante muchos siglos y no es nada nuevo, entonces esto en la actualidad ha evolucionado a lo largo del tiempo con la finalidad de perseguir y adaptarse a las nuevas realidades de un derecho moderno.

En la antigüedad, la perseguibilidad de un delincuente dependía en gran medida de la autoridad y el poder del afectado por el delito. Los ricos y poderosos tenían más posibilidades de hacer que se llevara a cabo una investigación y de obtener justicia por un delito cometido en su contra. Los pobres y sin poder, por otro lado, a menudo eran ignorados o tratados con menos consideración por las autoridades.

Con el tiempo, se han desarrollado sistemas legales más formales y justos para hacer cumplir la ley y perseguir a los delincuentes. En muchos países modernos, la perseguibilidad de un delincuente es independiente de la posición social o económica de la víctima y se basa en principios de igualdad ante la ley. Pero, todavía existen desigualdades y problemas que afectan

a varios lugares dando así un problema para realizar una correcta justicia y trato de equidad ante la ley en muchos lugares del mundo.

Algunos problemas que las autoridades en el transcurro del tiempo han enfrentado para una persecución del delincuente son:

1. **Falta de recursos:** En la antigüedad y en la actualidad, las autoridades a menudo carecen de los recursos necesarios y con esto para los nuevos problemas es la falta de capacidad o capacitaciones para entender la diferenciación y persecución de una persona digital la cual ha llevado a una persecución a veces errónea y esto ha llevada a un paraíso de impunidad para el sujeto activo. Los problemas pueden incluir lo que es la falta de personal, tecnología, financiación y capacitación.
2. **Testigos y pruebas:** Obtener testigos y pruebas suficientes para probar la culpabilidad de un delincuente puede ser un desafío y para probar la culpabilidad de los delincuentes informáticos es aún más difícil por el hecho de que la identificación del sujeto activo siempre permanece en el anonimato. Además, las pruebas pueden ser fácilmente destruidas o manipuladas en lo referente a los delitos informáticos, y que la prueba fundamental es el dispositivo informático es fácil alterar la información y con ello dificultar la presentación de la prueba.
3. **Corrupción y parcialidad:** La corrupción y la parcialidad en las autoridades pueden dificultar la persecución de los delincuentes. Si las autoridades están en un estado de imparcialidad a ciertos grupos o individuos, pueden no investigar adecuadamente a los delincuentes.
4. **Falta de leyes y normas claras:** En algunos lugares y épocas, las leyes y normas relacionadas con el delito y el castigo pueden ser confusas o incluso inexistentes y esto no ha sido una excepción en la actualidad, con esto me refiero que la falta de entendimiento de cómo funciona las nuevas herramientas modernas ha llevado a una generalización de algunos delitos. Esto puede dificultar la persecución de los delincuentes informáticos ya que, la generalización lleva a la impunidad a los delitos singularizados y por ende a un sistema penal ineficiente.
5. **Falta de cooperación internacional:** En la actualidad, los delincuentes a menudo cruzan fronteras para evitar la persecución, esto en referencia a los delitos comunes, para los delitos cibernéticos las fronteras no representan un problema para el sujeto activo para seguir con sus actividades. Si los países no

colaboran entre sí, puede ser difícil para las autoridades de un país perseguir a un delincuente que haya huido a otro país o se encuentre en el.

6. **Identificación del sujeto activo:** Bajo el contexto de los ciberdelitos, la identificación del sujeto activo (autor) en la actualidad es un desafío muy significativo, esto debido a la naturaleza misma de la tecnología usada para llevar a cabo las acciones, la misma llevada por el anonimato del internet esto llevado al uso de bots y técnicas de ocultamiento de identidad hacen que sea más difícil el rastreo a los responsables de los delitos cibernéticos.

   Entonces, concluimos que la identificación del sujeto activo en los delitos informáticos es un tema crítico y la parte más difícil al momento de llevar a la justicia al sujeto pasivo y el mismo se debe abordar de una manera diligente, entre los problemas para identificar al sujeto activo serían los siguientes: Anonimato, soberanía de los estados, falsificación de identidad o a su vez uso de identidades de terceros, uso de redes de bots y a su vez las diferentes técnicas de ocultamiento.

La persecución de delincuentes informáticos es un proceso complejo que involucra a diferentes agencias gubernamentales y organizaciones privadas ya que se trata de delitos transnacionales. A continuación, se presentan algunas características que se usan con más frecuencia en la persecución del delincuente informático.

Identificación del delito: La primera etapa más usada es la de determinar si se ha cometido un delito informático, en el caso de que se identifique el cometimiento del delito, se intenta identificar al sujeto activo.

Recopilación de pruebas: Una vez identificado el delito, como segunda etapa consistiría en reunir pruebas con la finalidad de demostrar la culpabilidad del sospechoso. Esto puede incluir la recopilación de registros de actividad del sistema, análisis de malware y otras técnicas .

Solicitud de orden judicial: para una tercera etapa, con la finalidad de llevar a cabo una investigación más a fondo se debe tener pruebas suficientes para demostrar la sospecha, con lo anteriormente dicho se vuelve una opción obtener una orden judicial para acceder a cierta información más específica y de carácter más personal.

Detención y procesamiento: Si se tiene suficiente evidencia para arrestar al sospechoso, y reuniendo los elementos de convicción se procederá a su detención.

Juicio: Si el sospechoso es declarado inocente, quedará en libertad. Si es declarado culpable, se le impondrá una pena acorde con la ley penal vigente del país en el cual ha sido juzgado.

Es importante tener en cuenta que cada caso es único y el proceso de persecución de un delincuente informático puede variar en función del caso en concreto, por ejemplo no es lo mismo perseguir a un sujeto activo con sospechas de phishing a uno con sospechas de ciberacoso, dadas que las circunstancias son específicas.

4.4.2. Reparación integral

La reparación integral en el derecho penal es un concepto que ha ido evolucionando a lo largo del tiempo. Inicialmente, el objetivo principal del derecho penal era la retribución o castigo del delito cometido. Sin embargo, a medida que la sociedad ha avanzado, también lo ha hecho la comprensión de que la justicia no solo se trata de castigar a los delincuentes, sino también de restaurar el daño causado y a su vez la reinserción de este a la sociedad mediante las cárceles.

En este sentido, la reparación integral en el derecho penal se refiere a la restauración de los derechos y bienes jurídicos afectados por el delito, tanto a nivel material como moral. Esto incluye la restitución de bienes, la indemnización por daños y perjuicios, la rehabilitación, la satisfacción, la garantía de no repetición y la reparación simbólica y si bien se habla de la reparación integral se me hace de suma importancia abordar los temas de la tipicidad y legalidad en el derecho penal.

Para comenzar el principio de tipicidad asienta las bases dentro de la sociedad donde los sistemas legales eran totalmente arbitrarios y por ende las autoridades se adjudicaban amplios poderes con el fin de imponer un castigo, en la mayoría de veces abusivo, a sus ciudadanos esto sin un marco penal legal claro, con lo anteriormente expuesto nace una idea, la idea de la creación un marco legal con el objetivo de la limitación del poder punitivo de un Estado para proteger los derechos individuales de las personas en una sociedad, entre las más importantes ventajas serian el conocer y a su vez comprender las leyes bajo las cuales se van a juzgar.

Entonces el principio de tipicidad es un concepto fundamental en materia del derecho penal, esta se refiere a que una conducta solo es considerada como delito si claramente está tipificada en la legislación penal (Código Orgánico Integral Penal), en otras palabras, para que

una persona puede ser condenada o juzgada por el hecho de haber realizado un delito la conducta se debe adecuar a lo que se establece en la norma penal.

El principio de tipicidad a su vez se relaciona con el principio de legalidad, entonces decimos que este principio también es llamado “nullum crimen sine lege penale” este establece que para que un delito pueda ser susceptible a un castigo debe existir una ley que lo establezca, en otras palabras, solo es susceptible una sanción a una persona por cometer una conducta delictiva si dicha conducta se encuentra tipificada como delito en la ley en el momento en que se comete el acto. Con lo anteriormente dicho, decimos que este principio es importante ya que sirve para la protección los derechos fundamentales de los individuos y evitar abusos de poder por parte del Estado, esto garantiza que las personas sean conscientes de lo que se considera delito y que a su vez no se les pueda condenar por comportamientos que no están expresamente prohibidos por la ley en el momento que ocurrieron.

Con todo lo anteriormente dicho se puede empezar a la explicación de la reparación integral para lo cual la historia de la misma, en América Latina, la reparación integral en el derecho penal comienza a ser contemplada en el año de 1990, y se incluye en algunos marcos legales de algunos países como lo son; Colombia, Chile, Argentina y México. Para establecer un ejemplo, en el país vecino, Colombia, en el año 2000, la Ley 600 la misma establece la conciliación en materia penal la misma que busca en su Art 42 la indemnización integral como una forma alterna de la pena o castigo.

La reparación integral, en el ámbito del derecho penal, el mismo se ha ido consolidando como el elemento clave para así alcanzar una justicia más justa y equitativa, que no solo busca castigar a los delincuentes, sino también restaurar los derechos y bienes jurídicos afectados por el delito tanto como sea posible.

En el ámbito del derecho penal, la reparación integral nos hace referencia a la restauración de los derechos y bienes jurídicos a los que haya sido afectados por el delito, este ya sea a un nivel material como moral. El mismo que incluye la restitución de bienes, y a su vez la indemnización por daños y perjuicios, la rehabilitación, la satisfacción, la garantía de no repetición y la reparación simbólica.

La reparación integral en el derecho penal no solo busca una restitución de los bienes materiales afectados, este también busca la reparación del daño moral causado a las víctimas y terceros afectados. Además, busca la prevención de la reincidencia del delito mediante la adopción de medidas como lo es la garantía de no repetición con el fin de evitar que se

produzcan nuevos delitos similares y a su vez es una herramienta fundamental para la justicia y la equidad, ya que busca restablecer los derechos y bienes jurídicos afectados por el delito, y garantizar que se adopten medidas para prevenir su repetición.

4.4.3. Reparación integral en el Código Orgánico Integral Penal

Como explicamos anteriormente la reparación integral es un forma de compensación a la víctima por parte del sujeto activo, en la legislación ecuatoriana la reparación integral se encuentra explicada en el Código Orgánico Integral Penal en su Art 77 el mismo que estipula que "La reparación integral radicará en la solución que objetiva y simbólicamente restituya, en la medida de lo posible, al estado anterior de la comisión del hecho y satisfaga a la víctima, cesando los efectos de las infracciones perpetradas. Su naturaleza y monto dependen de las características del delito, bien jurídico afectado y el daño ocasionado.

La restitución integral constituye un derecho y una garantía para interponer los recursos y las acciones dirigidas a recibir las restauraciones y compensaciones en proporción con el daño sufrido." (Codigo Organico Integral Penal , 2022, p, 30)

La reparación integral es un concepto amplio que busca abordar de manera completa los daños causados por una infracción o delito. En este sentido, se entiende que la reparación debe ser objetiva, es decir, que debe estar orientada a restablecer, en la medida de lo posible, el estado anterior a la comisión del hecho. Asimismo, debe ser simbólica, en el sentido de que debe reconocer y satisfacer las necesidades y demandas de la víctima.

La reparación integral no solo busca compensar el daño causado, este a su vez busca cesar los efectos de las infracciones perpetradas, lo cual significa que busca también prevenir que se produzcan nuevas lesiones en el futuro.

La restitución integral, como conclusión, se trata de un derecho de carácter constitucional para las víctimas, las mismas que tienen el derecho a interponer los recursos y acciones necesarias para recibir las restauraciones y compensaciones que les corresponden en proporción al daño sufrido. En este sentido, la reparación integral no sólo se trata de un mecanismo de justicia, también se basa en un derecho humano fundamental el mismo que busca que las victimas tengan una restauración digna en lo máximo posible del bien jurídico afectado.

Dentro del COIP se encuentras varios mecanismos de reparación integral los mismos que son:

Restitución: Este mecanismo se trata de devolver a la víctima, lo máximo posible, la situación anterior a la violación de sus derechos. Por ejemplo, si una persona ha sido

privada de su libertad, se busca restablecer su libertad y su derecho a la vida familiar y a la ciudadanía.

Rehabilitación: Este mecanismo se trata de la recuperación de las víctimas, tanto física como psicológicamente, y para ello se les brinda tanta atención médica como psicológica.

Indemnizaciones: Este mecanismo se trata de una compensación económica por el daño sufrido. Las indemnizaciones se basan en dos partes, por la primera los daños materiales en casos como la perdida de una propiedad, o a su vez inmateriales como los son los daños psicológicos y emocionales.

Medidas de satisfacción o simbólicas: Este mecanismo se trata de restablecer la dignidad de las personas afectadas y a su vez el reconocimiento de los daños causados. Por ejemplo, puede incluir disculpas públicas por parte de las autoridades responsables.

Garantías de no repetición: Este mecanismo se trata de la prevención en el marco de que no se vuelvan a repetir los hechos. Puede incluir medidas como lo es la capacitación de funcionarios públicos, y la creación de leyes y políticas públicas para prevenir futuras violaciones de derechos humanos, entre otras.

4.5.Persona digital

La persona digital es un concepto relativamente moderno que ha surgido con el desarrollo de la tecnología y la popularización de internet. A medida que cada vez más personas comenzaron a tener presencia en línea a través de redes sociales y otros medios, se desarrolló la idea de la persona digital como una forma de representar a una persona en el mundo digital.

Con el tiempo, la persona digital ha evolucionado y ha comenzado a incluir no solo información básica como nombre y fotografía, sino también elementos como intereses y actividades, información de contacto y historial laboral. También se ha vuelto cada vez más común utilizar la persona digital en el contexto de la realidad virtual y la inteligencia artificial, donde se puede utilizar para representar a una persona en entornos digitales.

La persona digital es un término que se refiere a la representación digital de una persona. Esto puede incluir su nombre, fotografías, información de contacto, historial laboral, intereses y cualquier otra información relevante. La persona digital se puede utilizar para presentar a una persona en línea, como en redes sociales, sitios web profesionales o plataformas de empleo.

También puede ser utilizada para representar a una persona en el contexto de la realidad virtual o la inteligencia artificial.

Pero con lo anteriormente dicho, ¿este término es de importancia? La respuesta es sí, bajo estos conceptos, si bien este término nuevo es la base misma de lo que es la actividad realizada en el mundo virtual y lo que cada persona refleja en la red sobre sí misma, decimos que para poder hablar de los delitos informáticos o cualquier tema relacionado con la virtualidad se necesita conocer que es una persona digital.

El doctor Vicente Vallejo nos dice que "…Es un modelo de individuo creado mediante la recopilación, almacenamiento y análisis de los datos sobre dicha persona…" (VALLEJO, 2010, pág. 13)

Decimos que la persona digital es una persona que ha sido creado a partir de otra para reflejar una de esta basada en su actividad en el ciberespacio, o bien se diría un espejo, en si la persona digital se crea a partir de información ya sea subida por el usuario (fotos, información, fechas, etc) ya sea en una red social, blog o a su vez la interacción con demás paginas distintas de internet, cabe decir que todo movimiento en la web es una adaptación más a tu concepto en la web

"…La persona digital es un modelo de la personalidad publica de un individuo, basado en los datos y mantenido por las transacciones y que ha sido concebido para ser utilizado en representación del individuo…" (VALLEJO, 2010, pág. 14)

Con lo anteriormente dicho, esta persona es una representación basada en datos recopilados de páginas que tiene como finalidad una representación del individuo en el ciberespacio

No obstante, este término es tan nuevo que incluso algunos autores lo denominan como identidad digital, así como:

la identidad digital está constituida por diferentes tipos de datos según el usuario tenga o no la intención de revelarlos, lo que da lugar a una identidad declarada, compuesta por aquella información que revela expresamente la persona, otra identidad actuante, según las acciones que esta lleva a cabo, y otra calculada o inferida, según el análisis de las acciones que realiza la persona. Toda esta información puede ser utilizada para configurar una idea de quién es y qué le gusta a una persona determinada. (Georges, 2010 citado en Fundación tecnologica, 2013, pág. 11)

La idea de la identidad digital es una serie de datos que son reunidos en base a lo que una persona sube ya sea que tenga o no intención de revelarlos, esto con el fin de construir una idea de que es y qué es lo que busca el usuario a quien le pertenezca esta información

De forma activa, se realiza aportando textos, imágenes y vídeos a Internet, participando, en definitiva, del mundo web. En los sitios de redes sociales, se construye a partir de un perfil de usuario, que a menudo se enlaza a perfiles de otros usuarios o contactos. Una identidad digital bien gestionada y homogénea con la identidad analógica no sólo repercute en una vida más activa en todos los ámbitos, sino que también tiende a consolidar un entramado social más sólido fuera de Internet. (GUIONES, 2010, pág. 3)

La aportación por parte de los internautas al mundo digital va desde la subida de fotos al simple hecho de buscar en un navegador (Google, opera, Firefox), con esto si bien es fácil construir una persona digital que represente a un ser que interactúa en ella también es instrumento de defraudación de identidad por la facilidad misma

En conclusión, la persona digital es un término que se refiere a la representación de un individuo en la era digital, incluyendo su información personal, interacciones en línea y actividades en Internet. La importancia de estudiar la persona digital radica en que permite entender cómo la tecnología y la informática están transformando la forma en que las personas se relacionan entre sí y con la tecnología, así como también cómo esto afecta a su privacidad, seguridad y autenticidad en línea. Además, el estudio de la persona digital es importante para informar la toma de decisiones sobre la política y la regulación en el espacio digital.

Su importancia en el derecho penal se centra en cómo la presencia y actividad en línea de un individuo puede ser relevante en la investigación y persecución de delitos en el espacio digital. Esto incluye cómo se pueden utilizar las pruebas digitales para demostrar la comisión de delitos como el fraude, la extorsión, la difamación y otros delitos relacionados con la tecnología.

Además, la persona digital también es relevante en el derecho penal porque puede afectar la privacidad y la seguridad de las personas en línea, y puede ser utilizada para cometer delitos como el acoso y la ciber violencia.

Por lo tanto, es importante estudiar la persona digital en el derecho penal para desarrollar leyes y regulaciones adecuadas que protejan los derechos y la seguridad de los ciudadanos en

el espacio digital, así como para establecer los procedimientos adecuados para la investigación y persecución de delitos en línea.

4.6.Ciberstalking

Al llegar al objeto de investigación primero quiero comenzar que, como dije en páginas anteriores, los delitos cibernéticos no son complicados ya que son delitos físicos que son llevamos a la virtualidad con esto quiero decir que este concepto parte de dos palabras la primera que es **ciber** que es un prefijo el mismo que se usa por los cibernautas para referirse a temas relacionado con redes, y por su otra parte **stalking** que es un término que lo explicaremos a profundidad.

El término "stalking" se popularizó en los Estados Unidos a principios de la década de 1990, cuando comenzaron a surgir casos de personas que acosaban y persiguieron a otras de manera persistente y peligrosa. Antes de esto, el comportamiento que hoy en día se conoce como stalking solía ser conocido como acoso o persecución. El concepto de acoso o "stalking" se ha desarrollado a lo largo de los siglos como una forma de comportamiento persistente y molesto dirigido hacia una persona. Aunque el acoso ha existido en diferentes formas a lo largo de la historia, el término "stalking" se popularizó en los años 90 en relación con el comportamiento obsesivo y perseguidor de ex parejas o personas conocidas.

En 1990, una mujer a quien un hombre había estado persiguiendo y acosando, fue asesinada. Este caso llamó la atención pública sobre la importancia de proteger a las víctimas de acoso y condujo a la aprobación de leyes estatales de "stalking" en los Estados Unidos. Desde entonces, el acoso ha sido reconocido como un problema serio a nivel mundial y muchos países han desarrollado leyes y regulaciones para proteger a las víctimas y perseguir a los acosadores.

Para explicar más a fondo lo que es el stalking citare a Alonso de Escamilla que nos dice que:

> La incriminación del stalking proviene de los Estados Unidos de América y tiene lugar en los años noventa. Con anterioridad a esta fecha diversos sucesos atrajeron la atención de los medios de comunicación por afectar a personajes muy conocidos. Así, el asesinato del cantante John Lennon a principios de los años ochenta o el de la actriz Rebecca Schaeffer, a finales de esa misma década. El asesinato de cuatro mujeres a manos de sus exmaridos en Orange County o las persecuciones y acosos a otras actrices como Jodie Foster o Theresa Saldana o a la cantante Madonna, causaron una gran conmoción en la sociedad americana. Hasta entonces solo algunos Estados tenían leyes que regulaban el

> harassment o assault, y que resultaban poco idóneas para proteger a estas víctimas de acoso. Esta situación y estos sucesos determinan que el Estado de California aprobara la pri- mera ley antistalking de los Estados Unidos de América en 1990. Esta decisión fue seguida por el resto del pais y ese mismo año se aprobaron leyes antistalking en más de treinta Estados. En 1993 los diecinueve Estados restantes lo hicieron también, así que en la actualidad los cincuenta Estados que integran la Confederación, más el Distrito de Columbia, tienen su correspondiente tipo penal. Como las respectivas leyes contemplaban de forma diferente el acoso, al que in- cluso denominaban de forma diferente (stalking, criminal harassment, criminal menace), en 1992 el Congreso de los Estados Unidos de América comisionó al National Institute of Justice para elaborar un Model Stalking Code que sirviera de patrón para los diferentes Estados, Código que ha sido recientemente modificado para adaptarlo a las nuevas formas de comisión de este delito, particularmente aquellas constituyen supuestos de ciberacoso. En 1996 el delito de stalking se con- virtió en delito federal y se incluyó en el United States Code ((ESCAMILLA, 2018, pág. 219)

La regularización del stalking, surgió en estados unidos país en que su definición exigía una conducta dirigida repetitivamente contra un individuo concreto que este experimente como intrusiva o no deseada y que le cause miedo o intimidación, entonces con lo antes acotado tenemos información de que va trata la figura delictiva denominada stalking y su importancia de estudio, a continuación, veremos una definición más precisa.

> El termino stalking, acuñado por el derecho anglosajón, se puede traducir como una conducta intencionada y maliciosa de persecución obsesiva (obssesional following), acecho o acoso respecto de una persona a que se convierte en objetivo. Constituye, por tanto, un patrón de conducta, una suerte de estrategia de hostigamiento anormal, de larga duración y que esta dirigida a una persona (ESCAMILLA, 2018, pág. 217)

Decimos que el termino stalking proviene de su propia historia, como se detalló anteriormente, y trata de un acercamiento no consentido de la víctima que le provoque miedo y que no le permita realizar sus actividades con normalidad, este si bien es solo el inicio de muchos otros delitos pero a su vez debe ser diferenciado ya que se puede confundir con "Grooming" que si bien no esta alejado de serlo su diferencia y actuación es muy diferente, es de muy importante diferenciarlo es por ello que detallare las características del mismo.

Si bien con esto podemos decir que las características o un patrón de conducta que sobresalen de esta figura delictiva es:

_ **Hostigamiento anormal de larga duración:** se refiere a un comportamiento repetitivo y negativo, como la intimidación o el acoso, que dura un período prolongado de tiempo y puede causar un impacto negativo en la salud mental y emocional de la persona afectada. Este comportamiento puede incluir una amplia gama de acciones, como mensajes ofensivos, rumores difamatorios, exclusiones sociales o cualquier otra forma de abuso emocional o psicológico.

_ **Acto manifestó de persecución a una persona, no querido y sentido como intimidatoria:** se refiere a un comportamiento intencional y repetitivo que causa un malestar emocional y psicológico en la persona afectada. Este comportamiento es considerado una forma de acoso y puede incluir acciones como intimidación, difamación, acoso en línea, exclusión social, entre otros.

Dependiendo de la gravedad y la naturaleza del comportamiento, puede ser considerado un delito y estar sujeto a consecuencias legales. Algunos de los delitos que podrían aplicarse en estos casos incluyen acoso, acoso escolar, difamación, amenazas, entre otros.

_ **Allanamiento de morada, efectuar falsas acusaciones, amenazas, acometer o asaltar a la víctima o retenerla:** Si bien esta característica tiene muchas cosas que explicar diremos que el allanamiento de morada se refiere a la entrada ilegal en una propiedad privada, como ya a sido explicado anteriormente, como una casa o un apartamento, sin el permiso de su propietario o habitante o en el caso de los delitos informáticos se refiere a acceso a dispositivos informáticos.

Efectuar falsas acusaciones significa hacer declaraciones falsas o maliciosas sobre alguien con el objetivo de dañar su reputación o su carrera.

Amenazas se refiere a hacer declaraciones o acciones que causen miedo o temor a otra persona, incluyendo la amenaza de daño físico o psicológico.

Elementos del stalking:

_Que se lleve a cabo una serie de actos concatenadas que constituyan un patrón de conducta, que sen de carácter no deseado (sin anuencia de la víctima)

_ Produzca sentimientos de temor que impida llevar una vida normal

Con estas características podemos diferenciar sobre los diferentes tipos de acoso, y de diferentes tipos de ciberdelitos que existen, y por esta razón que es necesario su diferenciación para dar una importancia en su estudio y en su necesaria tipificación.

Esto como introducción a lo que es el stalking, entonces, decimos que el ciberstalking (así como muchos otros ciberdelitos) es consecuencia de la misma era digital, si bien el avance no es malo desde el descubrimiento del petróleo no hemos hecho más que avanzar sin medir consecuencias, con esto quiero llegar a que actualmente como estamos viviendo apenas el inicio de esta nueva solo estamos probando el inicio de los muchos problemas que nos tiene esta nueva era y me atrevo a decir que muchos de ellos no serán resueltos nunca, es por esto que los problemas que se pueden resolver o controlar como son los delitos cibernéticos los mismos que son un problema por su anonimato y una leve o casi inexistente ley penal y cooperación internacional será un problema muy largo en resolver.

Pero, con el avance de la tecnología y la popularidad de Internet, el acoso en línea, también conocido como "ciberstalking", se ha convertido en un problema cada vez más prevalente y ha requerido un enfoque adicional para abordarlo, es por ello que tratare de definirlo y realizar cuáles son sus nuevas características.

> Conducta de acoso u hostigamiento repetitivo que se lleva a cabo en contra de la voluntad de la víctima, utilizando algunas de las herramientas que proporciona internet, como son email-s, chat, mensajes de texto, WhatsApp, redes sociales como Facebook o Twitter, web Pages, o cualquier otro medio de ciberstalking (ESCAMILLA, 2018, pág. 229)

Si bien, la conducta del cibersalking es el acecho, persecución obsesiva que la víctima no la quiera la misma que le provoca daños psicológicos incluso físicos, el mismo acoso se da desde las redes sociales, entonces concluimos que es un comportamiento repetitivo y no deseado que se realiza a través de internet o dispositivos móviles. Incluye la utilización de emails, chats, mensajes de texto, redes sociales, páginas web y cualquier otro medio electrónico para hostigar a una persona en contra de su voluntad. Es una forma de abuso digital que puede tener graves consecuencias para la víctima y puede ser perjudicial para su salud mental y bienestar.

> El término “cyberstalking” hace referencia al uso de Internet, ordenador o cualquier otra tecnología de la comunicación para acosar u hostigar a una persona. Como modalidad de stalking (GREGORIE, 2001, pág. 1)

Cyberstalking es una forma de acoso en línea que se lleva a cabo a través del uso de tecnologías de la información y la comunicación (TIC). Se trata de un comportamiento repetitivo y no deseado que puede incluir el monitoreo, amenazas, difamación, suplantación de identidad y otros actos intimidatorios realizados a través de internet. Es una forma de hostigamiento digital que puede ser muy dañina para la víctima, y puede afectar su bienestar y su seguridad.

> Se trata de mensajes reiterados y a largo plazo hacia una persona que se elige como blanco, utilizando para ello todos los canales de comunicación, ya sean privados, como es el correo electrónico o los mensajes de celular, o públicos, como muros de redes sociales, chats, foros de discusión o incluso a través de videojuegos on-line. Debido a su frecuencia y repetitividad, a los acosadores que utilizan esta forma de ciberbullying se les ha dado el nombre de atormentadores. Los mensajes pueden tener contenidos ofensivos verbales o de tipo visual. (REYNOSO, 2014, pág. 21)

El cyberstalking es una forma de acoso repetitivo y persistente que se realiza a través de internet o dispositivos móviles. Los acosadores envían mensajes repetitivos y ofensivos a través de diversos canales de comunicación, incluyendo correo electrónico, mensajes de texto, redes sociales, foros de discusión y videojuegos en línea. Esta forma de acoso puede tener graves consecuencias para la víctima, incluyendo daño emocional y estrés.

El ciberacoso implica el uso de las tecnologías de la información y la comunicación como plataforma de una conducta intencional, repetida y hostil de un individuo o de un grupo para hacer daño a otros (ORTEGA, 2016, pág. 19)

El ciberacoso es una forma de acoso digital que se realiza a través del uso de tecnologías de la información y la comunicación. Esta conducta implica el uso intencional y repetido de medios electrónicos para hostigar y hacer daño a otras personas. El ciberacoso puede incluir una variedad de acciones, como el acoso en línea, el sexting, la difamación en línea, la suplantación de identidad y otras formas de hostigamiento en línea.

Características del nuevo stalking en el ciberespacio

Si bien ya sabemos que es el cibersaltking no podemos olvidarnos ¿Qué diferencia el ciberstalking de otros delitos? Pues para contestar esta interrogante decimos que para Alonso de Escamilla las características de esta nueva modalidad delictiva son:

1.- El anonimato que proporciona la red, y que sirve como pretexto para que el lenguaje del acoso cibernético se mucho más directo o violento que el que se usa en la vida real: El anonimato que proporciona Internet puede ser un factor importante en el ciberstalkning, ya que permite a los acosadores actuar sin ser identificados y, por lo tanto, puede hacer que su lenguaje y comportamiento sean mucho más directos y violentos que en la vida real. La sensación de impunidad que proporciona el anonimato puede alentar a los acosadores a utilizar un lenguaje más agresivo y ofensivo, y a perpetrar actos más graves de acoso. Es importante recordar que, aunque la persona acosadora esté detrás de una pantalla, sus acciones tienen consecuencias reales para la víctima y deben ser tomadas en serio.

2.- La situación de poder en la que se encuentra el acosador, gracias a ese anonimato del que goza, y que pueda utilizar tanto respecto de personas que ya conoce, como de aquellas a las que conoce a través de chats o foros de la más variada naturaleza: El anonimato que proporciona Internet puede dar a los acosadores una sensación de poder y control sobre sus víctimas, ya que pueden actuar sin ser identificados. Este poder les permite acosar tanto a personas que conocen en la vida real, como a aquellas que conocen a través de chats o foros en línea. Además, el hecho de que el acosador pueda actuar desde la distancia y sin enfrentarse a las consecuencias de sus acciones en persona, puede aumentar su sensación de poder.

3.- La importante información que puede recibir el acosador de la propia víctima a través de sus perfiles, información que puede referirse a su vida personal o privada y que resulte fundamental para el Stalker: Los perfiles en línea y las redes sociales pueden ser una fuente de información para los acosadores. La información personal que las víctimas comparten en línea, como su lugar de trabajo, su ubicación, su historial de relaciones y su vida privada, puede ser utilizada por los acosadores para perseguir y acosar a sus víctimas. Esta información puede resultar valiosa para los acosadores, ya que les permite tener un mayor control y conocimiento sobre sus víctimas, lo que aumenta su capacidad para dañar a estas personas.

4..- La circunstancia de que es la propia red la que proporciona los diferentes medios que utiliza el stalker. Sirva como ejemplo el envío de mensajes online, de contenido variado (insultante, amenazante) y de cadencia variable, sistemática o masiva (mail bombing). Dichos envíos de e-mail pueden ser de carácter anónimo, a través de e-mail gratuito, por ejemplo, o manipulados para que parezcan enviados por la propia víctima,

lo que puede colocarla en muy difícil situación. La red y las tecnologías de la información y la comunicación proporcionan a los acosadores una amplia gama de medios para acosar y hostigar a sus víctimas. Un ejemplo de esto es el envío masivo de correos electrónicos con contenido insultante o amenazante. Estos correos electrónicos pueden ser enviados de forma anónima, a través de un correo electrónico gratuito, o pueden ser manipulados para aparecer como si fueran enviados por la propia víctima. Esto puede poner a la víctima en una situación muy difícil, ya que puede ser vista como responsable de los correos electrónicos o ser acusada de enviarlos. El uso de estos medios por parte de los acosadores agrava la situación de la víctima y puede ser perjudicial para su bienestar físico y psicológico.

5.- La posibilidad de manipular fotografías o imágenes de la víctima que se encuentren en Internet y que hayan sido facilitadas por ella misma en alguna de sus redes sociales o chats. Otra posibilidad puede ser colgar contenidos ofensivos dedicados a la víctima o utilizar servicios de mensajes (sms) desde la red, pues no pueden identificarse fácilmente: El ciberacoso también puede incluir la manipulación de fotografías o imágenes de la víctima que se encuentran en internet, así como la publicación de contenido ofensivo o el uso de servicios de mensajes (sms) a través de la red que no pueden ser fácilmente identificados, lo que aumenta el poder del acosador sobre la víctima.

Bienes jurídicos protegidos que se vulneran en el ciberstalking

Dignidad: La dignidad en derecho penal se refiere al valor y respeto que se le reconoce a cada persona como ser humano, independientemente de su condición o situación. En este contexto, la dignidad humana se convierte en un límite a la acción del Estado y de los particulares, y su protección se considera un elemento fundamental en el desarrollo de un sistema penal justo y humano.

> El derecho de la dignidad, en la legislación ecuatoriana, según el artículo 84 de la Constitución de la Republica del Ecuador, en el titulo III capitulo primero, de las garantías constitucionales estipula: La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución. (Ecuador, 2008, pág. 34)

Integridad moral: La integridad moral se refiere a la integridad o pureza de los valores y principios éticos y morales de una persona. Es la coherencia y consistencia entre lo que se dice y lo que se hace, y se basa en la honestidad, la rectitud y la responsabilidad en las acciones y decisiones diarias. La integridad moral se considera un elemento fundamental para la construcción de una sociedad justa y respetuosa.

En la legislación ecuatoriana, según el artículo 66 de la Constitución de la Republica del Ecuador, en el capítulo sexto, de los derechos de libertad en su numeral 3 estipula: El derecho a la integridad personal (Ecuador, 2008, pág. 26)

Intimidad: La intimidad personal es un derecho fundamental protegido por el derecho que consiste en el derecho a la privacidad y a la protección de la vida privada de una persona. La intimidad personal comprende aspectos como la vida sexual, las opiniones políticas y religiosas, las relaciones familiares y de amistad, así como también la información personal y la correspondencia.

En derecho, la intimidad personal es considerada un derecho inviolable y es protegida por la Constitución y diversas leyes internacionales de derechos humanos.

En la legislación ecuatoriana, según el artículo 66 de la Constitución de la Republica del Ecuador, en el capítulo sexto, de los derechos de libertad en su numeral 20 estipula: “El derecho a la intimidad personal y familiar”. (Consitución de la Republica del Ecuador, 2008, pág. 27)

Como conclusion decimos que, si bien los bienes protegidos estan enmarcados en la constitucion, este tipo de delito cibernetico solo a quedado en el estudio para su pronta o tardia incorporación, entonces si tenemos los bienes que se deben proteger y la conducta no esta regulada es el Estado quien esta fallando en su pronto reconocimiento.

Sujeto activo y sujeto pasivo en el ciberstalking

Para comenzar con la explicación de las características y cuáles son las partes de esta figura delictiva se me hace menester conceptualizar estos dos conceptos.

En todo delito ya sea en el mundo físico o digital siempre van a tener dos partes el sujeto pasivo (Que es aquel que realiza el hecho delictivo) y el sujeto acivo (es el tutelar del bien jurídico protegido como son dignidad, integridad mora, etc)

Sujeto activo

El sujeto activo es un concepto dogmático que precisa cualidades que debe reunir una persona al momento de cometer la conducta delictiva; es el agente que realiza la acción y omisión descrita por el tipo penal. (VILLVICENCIO, 2017, pág. 67)

El sujeto es la persona o entidad que comete un delito, es decir, la persona que realiza la acción delictiva. El sujeto activo es responsable de la acción delictiva y, por lo tanto, es el principal objeto de la persecución penal.

El sujeto activo puede ser una persona natural o jurídica y puede cometer un delito de forma individual o en conjunto con otros sujetos, este también ess un elemento esencial en el derecho penal, ya que es el autor de la acción delictiva y, por lo tanto, es el que debe ser perseguido y sancionado en caso de ser declarado culpable. Además, el sujeto activo tiene derechos y garantías en el proceso penal, como el derecho a un juicio justo y a la presunción de inocencia.

En resumen, el sujeto activo es un concepto clave en el derecho penal que se refiere a la persona o entidad que comete un delito y que, por lo tanto, es el principal objeto de la persecución y sanción penal.

Sujeto pasivo

El sujeto pasivo es el titelar del bien jurídico tutelado, es el agente que recibe el comportamiento por acción o omisión realizada por el sujeto activo. El sujeto pasivo puede ser tanto la persona física imputable o no imputable como la persona jurídica, la sociedad o el Estado. (VILLVICENCIO, 2017, pág. 68)

El sujeto pasivo en el derecho penal es aquella persona o entidad contra la cual se comete un delito. Es decir, es la víctima o el objeto de la acción delictiva. El sujeto pasivo puede ser una persona natural o jurídica y puede ser afectado de diversas formas por el delito.

Es importante destacar que el sujeto pasivo en el derecho penal no solo se refiere a las personas, sino también a entidades como el Estado, la sociedad o el medio ambiente, que pueden ser afectados por ciertos delitos como la corrupción, el terrorismo o la contaminación.

En un proceso penal, el sujeto pasivo es considerado como la parte afectada por el delito y tiene derecho a ser informado y a participar en el proceso. Además, en muchos casos el sujeto pasivo puede reclamar una reparación por el daño sufrido en el proceso penal o en un procedimiento civil separado.

En resumen, el sujeto pasivo es un elemento fundamental en el derecho penal, ya que representa la parte afectada por la acción delictiva y tiene derechos y protecciones específicas en el proceso penal.

Sujeto activo y pasivo en el ciberstalking

Con lo anterior mente dicho de los sujetos que participan como lo es el sujeto activo y pasivo, es lo mismo en los ciberdelitos, pero aplicados en este tema de investigación decimos que el sujeto activo es la persona que lleva a cabo la acción de acosar o hostigar a otra persona a través de medios electrónicos o tecnológicos, como internet, redes sociales o mensajes de texto. Este sujeto activo puede realizar acciones como el envío de mensajes intimidatorios, la difusión de información personal o falsa, o el acoso constante a través de las redes sociales.

Por otro lado, el sujeto pasivo es la persona o individuo contra el que se comete el ciberacoso. Esta persona puede sufrir daños emocionales, psicológicos o incluso físicos como resultado del acoso y la hostigación por parte del sujeto activo llegando así por el recibimiento de mensajes del parte del sujeto activo los mismos que llegan a causarle incomodidad o incluso llegar a sentir miedo.

Es importante destacar que tanto el sujeto activo como el pasivo pueden ser de cualquier edad, género o procedencia, y que el ciberacoso puede tener graves consecuencias para la salud y el bienestar de la víctima, pero se me hace de importancia aclarar que este delito se da con mayor frecuencia en los jóvenes, donde la mayoría de los autores o sujeto activo son de género masculino y a la persona que se comete el ciberacoso o sujeto pasivo en su gran mayoría es de género femenino.

Elementos del tipo penal

Sujeto activo: El sujeto activo puede ser cualquier individuo que utilice medios como redes sociales, correos electrónicos, mensajes de texto, aplicaciones de mensajería, blogs o cualquier otra forma de comunicación electrónica para acosar a la víctima. Pueden ser conocidos, desconocidos o incluso personas cercanas a la víctima, como exparejas o conocidos que buscan acosarla y perturbar su vida personal o profesional. (General)

Sujeto pasivo: La persona que está siendo objeto de acoso, hostigamiento o persecución a través de medios electrónicos o digitales. En otras palabras, es la víctima del ciberstalking. El sujeto pasivo puede ser cualquier individuo que esté siendo objeto de este tipo de conductas no deseadas y perturbadoras. (Especifico)

Objeto material: La persona o entidad que está siendo acosada, hostigada o perseguida a través de medios electrónicos.

Objeto formal o jurídico: La intimidad, la dignidad personal, la seguridad o la tranquilidad de la víctima.

Conducta típica: es el acoso, hostigamiento o persecución de una persona a través de medios electrónicos o digitales.

4.7.Derecho comparado

Antes de empezar a hacer un derecho comparado quiero aclarar que las leyes usadas en este apartado fueron traducidas al español ya que los países que tienen regulada esta conducta son de habla inglesa, con esto en mente decimos que:

4.7.1. Ciberstalking en la legislación de la República de los Estados Unidos de América

Para partir recordemos que como lo dije anteriormente Estados Unidos fue el epicentro donde fue la creación de stalking o antes su nombre llamado “Assault”, bien bajo este contexto este conceto se ha ido adaptando a las realidades sociales que viven en estados unidos, pero recordemos que Estados unidos son varios estados y por ende cada uno tiene diferentes leyes, entonces en California el ciberestalking se encuentra tipificado en el código penal de california, sección 646,9 en el mismo que nos dice lo siguiente:

> (a) Cualquier persona que intencional, maliciosa y repetidamente siga o acose intencional y maliciosamente a otra persona y que haga una amenaza creíble con la intención de poner a esa persona en un temor razonable por su seguridad, o la seguridad de su familia inmediata es culpable del delito de acecho, punible con prisión en una cárcel del condado por no más de un año, o con una multa de no más de mil dólares ($ 1,000), o con esa multa y prisión, o por prisión en la prisión estatal.

Si bien en este artículo de la ley y articulo citado nos dice que la actitud de acecho que tenga una intención maliciosa y repetitiva y la parte más interesante que nos señala que sus actuaciones tengan una amenaza la cual provoque un miedo razonable dando así la característica y actuación del Stalker, pero la pregunta en que parte nos remarca el uso de los medios electrónicos, este está señalado en el mismo artículo en el literal g y h al cual citaremos:

> (g) A los efectos de esta sección, "amenaza creíble" significa una amenaza verbal o escrita, incluida la realizada mediante el uso de un dispositivo de comunicación

electrónica, o una amenaza implícita en un patrón de conducta o una combinación de declaraciones y conductas comunicadas verbalmente, escritas o electrónicamente, hechas con la intención de colocar a la persona que es el objetivo de la amenaza en un temor razonable por su seguridad o la seguridad de su o su familia, y hecha con la aparente capacidad de llevar a cabo la amenaza de manera que la persona que es el objetivo de la amenaza tema razonablemente por su seguridad o la seguridad de su familia. No es necesario probar que el acusado tenía la intención de llevar a cabo la amenaza. El encarcelamiento actual de una persona que hace la amenaza no será un impedimento para el enjuiciamiento en virtud de esta sección. La actividad protegida constitucionalmente no está incluida en el significado de "amenaza creíble".

(h) Para los propósitos de esta sección, el término "dispositivo de comunicación electrónica" incluye, pero no se limita a, teléfonos, teléfonos celulares, computadoras, grabadoras de video, máquinas de fax o buscapersonas. "Comunicación electrónica" tiene el mismo significado que el término definido en la Subsección 12 de la Sección 2510 del Título 18 del Código de los Estados Unidos.

Dando así una tipificación a la figura delictiva ciberstalking dentro del código penal de California, es bastante importante recalcar que las características más importantes que se hacen alusión serian que las siguientes:

_Dando las palabras “cualquier persona” nos da a entender que el sujeto activo es de un carácter general con esto quiero decir que no se detalla ni genero ni grado de conocimiento en cualquier rama, entonces, se dice que el sujeto activo puede tener o no habilidades informáticas, pero esto no reduce el daño causado.

_Dando la utilización de la palabra “otra persona” estaría hablando de la persona que está siendo acosada o perseguida en el delito de ciberstalking. Por lo tanto, cuando se dice "a otra persona" en relación al sujeto pasivo, se está hablando de la víctima directa del delito, Entonces decimos que el sujeto pasivo puede ser general ya que puede ser cualquier persona y no una en especial dado que si bien el acoso en la mayoría de los casos es objetivo no se puede ignorar los casos que él acoso es aleatorio con finalidades de provocar daño.

_Dando la utilización de “amenaza creíble”, una amenaza creíble puede ser cualquier comunicación que un acosador hace a su víctima, ya sea verbalmente, por escrito o a través de medios electrónicos como es el objeto de estudio acrualmente, que sugiere que la persona podría sufrir daño o peligro. Por ejemplo, una amenaza creíble puede ser una

declaración explícita de violencia o una insinuación velada de que el acosador podría hacer daño a la víctima o a alguien cercano a ella. La evaluación de si una amenaza es creíble dependerá de las circunstancias específicas del caso, dando así inicio a la figura de estudio.

4.7.2. Ciberstalking según la legislación de Reino Unido

La figura del ciberstalking se encuentra en la sección segunda de la ley de delitos informáticos de 2013 del Reino Unido que nos dice:

> 2. Actos de hostigamiento
>
> (1) Cualquier persona que envíe comunicaciones electrónicas con el propósito de causar ansiedad o miedo a la persona que las recibe, o para causar malestar grave o molestia a esa persona, comete un delito si:
>
> (a) su conducta se lleva a cabo de manera persistente y no deseada, y
>
> (b) su conducta tiene el efecto de cumplir uno de los siguientes criterios:
>
> (i) causar ansiedad o miedo a la persona que las recibe, o
>
> (ii) causar malestar grave o molestia a la persona que las recibe.
>
> (2) Se considerará que la conducta se lleva a cabo de manera persistente si se realiza en dos o más ocasiones.
>
> (3) Es una defensa para una persona acusada de delito en virtud de esta sección demostrar que su conducta estaba justificada o que tenía derecho a enviar las comunicaciones.
>
> (4) Una persona culpable de un delito en virtud de esta sección es responsable de un delito y es susceptible de una multa y/o pena de prisión por un plazo máximo de seis meses

La Ley de Delitos Informáticos de 2013 del Reino Unido, Sección 2, establece que es un delito cometer actos de hostigamiento en línea. En particular, la Sección 2 establece que es ilegal enviar comunicaciones electrónicas que son amenazantes o que causan ansiedad, angustia o miedo a la persona que las recibe.

Además, la Sección 2 también prohíbe el envío de comunicaciones electrónicas que son indecentes o que causan un malestar grave o molestia a la persona que las recibe. Estas prohibiciones se aplican a cualquier forma de comunicación electrónica, incluyendo correo

electrónico, mensajes de texto, publicaciones en redes sociales y cualquier otra forma de comunicación en línea.

La Sección 2 también establece que es un delito cometer actos de hostigamiento cibernético dirigidos a una persona específica o a un grupo de personas. El hostigamiento cibernético se define como un comportamiento que causa miedo o angustia a la persona que lo recibe, y que se lleva a cabo de manera persistente y no deseada.

4.7.3. Ciberstalking según la legislación de España

La Ley de Protección Integral contra la Violencia de Género de 2015 de España incluye la Sección 172 ter en el Código Penal que se refiere al delito de acoso u hostigamiento a través de las tecnologías de la información y la comunicación (TIC) que nos dice que:

> **1** el que acose a una persona a través de las tecnologías de la información y la comunicación, o por cualquier otro medio, con una finalidad que atente contra la dignidad de la persona, o con la finalidad de coartar su libertad o de generar un entorno intimidatorio, hostil, degradante, humillante u ofensivo, será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses.
>
> **2** será castigado con la pena de prisión de seis meses a dos años o multa de seis a
>
> veinticuatro meses si la conducta prevista en el apartado anterior se lleva a cabo contra una mujer por razón de su género.
>
> **3.** A los efectos de este artículo, se entenderá que se produce acoso cuando se realice un seguimiento o vigilancia persistente de la persona, cuando se recopile información de la persona sin su consentimiento, cuando se utilice la información obtenida para acosar a la persona, cuando se envíen mensajes no solicitados con contenido sexual o cuando se envíen mensajes que contengan amenazas o información que atente contra la dignidad de la persona.
>
> **4** A las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder por los delitos de calumnias, injurias, coacciones, amenazas o cualquier otro delito que pudiera cometerse en el marco del acoso a través de las tecnologías de la información y la comunicación.

Dando así otro concepto del ciberstalking, pero esta tiene una característica que los otros países no, el cual es significativo el cual es el endurecimiento de la sanción de acuerdo a su género, si bien en las encuestas que se realizaron se verifica que este es una figura delictiva que

en su generalidad el sujeto pasivo o víctima es del género femenino me parece una decisión acertada para su prevención.

Entonces decimos que se castiga a quien realice un seguimiento o vigilancia persistente de una persona a través de las TIC, recopile información sin su consentimiento, utilice esa información para acosarla, envíe mensajes no solicitados con contenido sexual o envíe mensajes que atenten contra la dignidad de la persona, con la finalidad de atentar contra su dignidad, coartar su libertad o generar un entorno intimidatorio, hostil, degradante, humillante u ofensivo.

Este artículo busca proteger la dignidad y libertad de las personas en el entorno digital y garantizar que las TIC no sean utilizado para acosar o hostigar a otros. Además, se establece una pena de prisión o multa en función de la gravedad de la conducta y de si se comete contra una mujer por razón de su género, con el fin de prevenir y sancionar este tipo de conductas delictivas.

5. Metodología

5.1. Materiales utilizados

Los materiales utilizados durante el desarrollo del presente trabajo de investigación curricular, han servido de apoyo académico con el fin de cumplir con los objetivos propuestos en el presente proyecto de investigación, recogiendo fuente bibliográficas como: Obras jurídicas, leyes, manuales, diccionarios, ensayos, revistas jurídicas, obras científicas y páginas web de los organismos de los diferentes Estados que se encuentran citados de manera idónea, formando para de las fuentes bibliográficas. Entre otros materiales que se han utilizado, se encuentran la computadora portátil, teléfono celular, retroproyector, cuaderno de anotaciones, conexión a internet, impresora, hojas de papel bond, fotocopias, anillados, impresión de borradores de tesis y empastados de la misma, entre otros.

5.2.Métodos

Los métodos son aquel conjunto de procesos y procedimientos que permiten el desarrollo y ejecución del proyecto de integración curricular, para ello durante el proceso de investigación socio - jurídico, se aplicaron los siguientes métodos:

Método Científico: Es una serie de etapas que hay direccionar de manera oportuna para obtener un conocimiento válido desde el punto de vista científico; este método fue utilizado al momento de analizar las obras jurídicas, científicas, desarrolladas en mi trabajo de investigación dentro de la revisión de literatura que comprende el marco conceptual y doctrinario, cuyos datos complementarios constan en las citas y bibliografía correspondiente.

Método Inductivo: Es un método que va de lo particular a lo general; este método permitió analizar la persona jurídica ya que primero se analizó un concepto particular que fue el concepto para luego llevar sus conceptos en ámbito internacional y por ende su función en el mundo virtual

Método Deductivo: Este método parte de lo general a lo específico; fue aplicado en el desarrollo de la investigación al analizar los diferentes tipos de conceptos como fue el derecho penal dando asi que partimos de lo básico como lo es el derecho penal y así llevándolo a algo especifico como lo es el derecho penal en el ciberespacio y a su vez usdo en el análisis de la figura “ciberstalking”

Método Analítico: Se utilizó este método cuando se realizó el análisis y comentario de cada una de las citas constantes en el Revisión de Literatura que comprende el marco

conceptual, doctrinario y derecho comparado; también fue aplicado al analizar e interpretar los resultados de las encuestas y entrevistas.

Método Exegético: Método empleado al momento de analizar las normas jurídicas utilizadas para la fundamentación legal del trabajo de investigación, estas son: Constitución de la República del Ecuador y las normas jurídicas en el derecho comparado.

Método Hermenéutico: Este método permite interpretar textos jurídicos, que permiten entender el sentido de las normas jurídicas, este método se aplicó en la interpretación de las normas jurídicas, en que se procede a realizar la interpretación de las leyes ecuatorianas pertinentes.

Método Mayéutica: Es un método de investigación que consiste en aplicar una serie de interrogantes a través de las cuales se va a descubrir conceptos que estaban ocultos en la mente del interrogado; este método se aplicó en las encuestas y entrevistas para lo obtención de información relevante para el desarrollo de la investigación.

Método comparativo: Este método permite contrastar dos realidades legales, mismo que fue aplicado en el desarrollo de la investigación a través del Derecho Comparado, en el cual se procedió a comparar la realidad jurídica ecuatoriana en códigos como lo son el Código orgánico integral penal o en otros estados solo código penal en países como España, Estados Unidos y Reino Unido obteniendo resultados en razón de las semejanzas y diferencias de estos ordenamientos jurídicos.

Método estadístico: El método estadístico permite recolectar datos cuantitativos o cualitativos de la investigación mediante el uso de las técnicas de la Entrevista y la Encuestas, aplicado al momento de realizar la tabulación, cuadros estadísticos, representación gráfica para desarrollar el punto de Resultados de la Investigación.

Método sintético: Consiste en resumir y unir los aspectos más relevantes dentro de la investigación. Este método fue empleado en todo el trayecto de la elaboración del trabajo de investigación; especialmente con la discusión de la verificación de objetivos, contrastación de hipótesis y fundamentación jurídica del proyecto de reforma legal, aplicando al momento de emitir un criterio luego de realizar un estudio minucioso de la temática.

6. Resultados

6.1. Resultado de la encuesta

La presente técnica de la encuesta fue aplicada dentro de la población estudiantil, la misma que fue la esencial para abarbar el objetivo específico número uno ya que al momento de encuestar una parte de la población es el momento de ver si el tema de investigación es importante para solucionar o estudiar un problema actual.

Primera pregunta

¿Conoce cuál es el significado del ciberstalking?

Tabla estadística #1

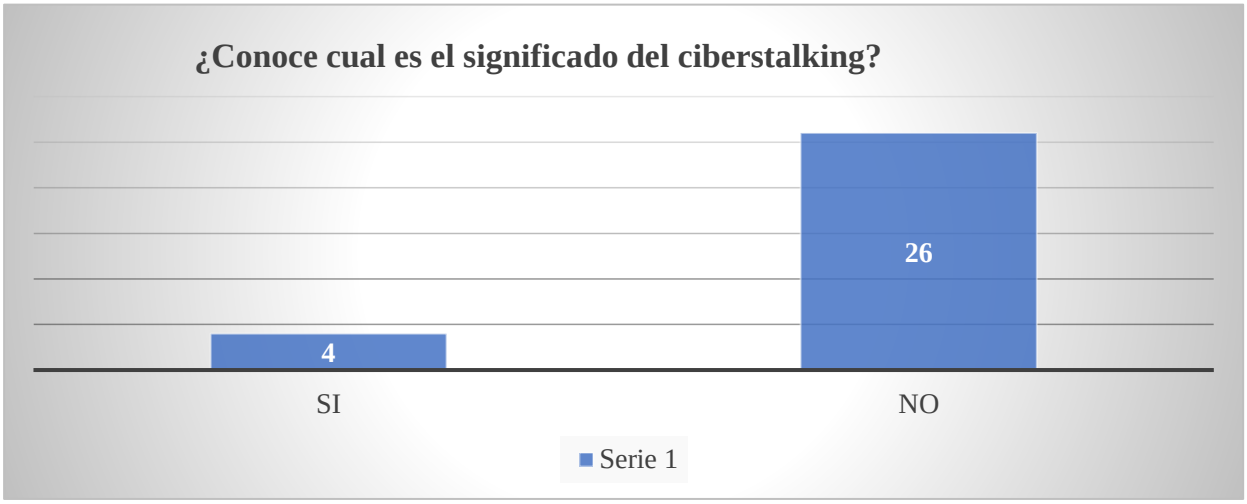


Figura 1 Significado del ciberstalking

Fuente: Sector estudiantil de la ciudad de Loja.

Autor: Miguel Angel Benitez Guayllas.

INDICADORES	VARIABLES	PROCENTAJES
SI	4	13,3%
NO	26	86,7%
Total	30	100%

Tabla 1 Significado del ciberstalking

Interpretación:

En la presente pregunta 4 personas han respondido que conocen el significado de esta figura delictiva el cual consiste en un 13,3% de los encuestados, que si bien no es un porcentaje alto, pero si uno considerable dado que el conocimiento de esta actividad delictiva no es muy conocida por el hecho de su reciente estudio, no me voy a explayar mucho en los que conocen porque no debería ser una sorpresa la información que es responsabilidad neta del estado.

Por su contraparte, 26 de los encuestados los mismos que equivalen al 86,7%, lo cual es un porcentaje muy alto y a la vez desalentador dada que la desinformación social existe y es por esto que este tema de investigación es importante para que se dé a conocer a la sociedad esta nueva figura que en la actualidad es tan común y a la vez tan normalizada, no agregue un "Porque" dado que si desconocen el termino, es algo muy contraproducente decir que fundamenten algo que no conocen, pero con esto quiero llegar que al Estado no solo sirve como ente firmador de convenios como fue con Budapest el mismo también es responsable que en su estado y enmarcado en su soberanía de capacitaciones tanto adultos y especialmente enfatizados en los jóvenes o como los llaman en los libros los "nativos digítales".

Análisis

No puedo estar de acuerdo con ninguna de las dos partes ya que es una pregunta para saber el conocimiento del tema a investigar, pero como un análisis diría que el estado como ente responsable la educación de su población citando que en la legislación ecuatoriana, según el artículo 26 de la Constitución de la Republica del Ecuador, en el capítulo segundo, de los derechos del buen vivir, en su sección quinta de educación estipula: "La educación es un derecho de las personas a lo largo de su vida y un deber ineludible e inexcusable del Estado. Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir. Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo.". (Conctitucion de la Republica del Ecuador, 2008, pág. 14) La educación es vista como un derecho fundamental y un medio para mejorar la vida de las personas y el bienestar de la sociedad en su conjunto. Por lo tanto, es esencial que el estado cumpla con su papel en la provisión de una educación de calidad a todos sus ciudadanos.con esto quero decir que si bien la autoeduccion es una base de partida el ser indivual y no se puede culpar al estado de la ignoracia del pueblo en su totalidad, no se puede negar la responsabilidad del estado ya que dadas los datos anteriormente expuestos de verifica el desconocimiento en temas de interes y

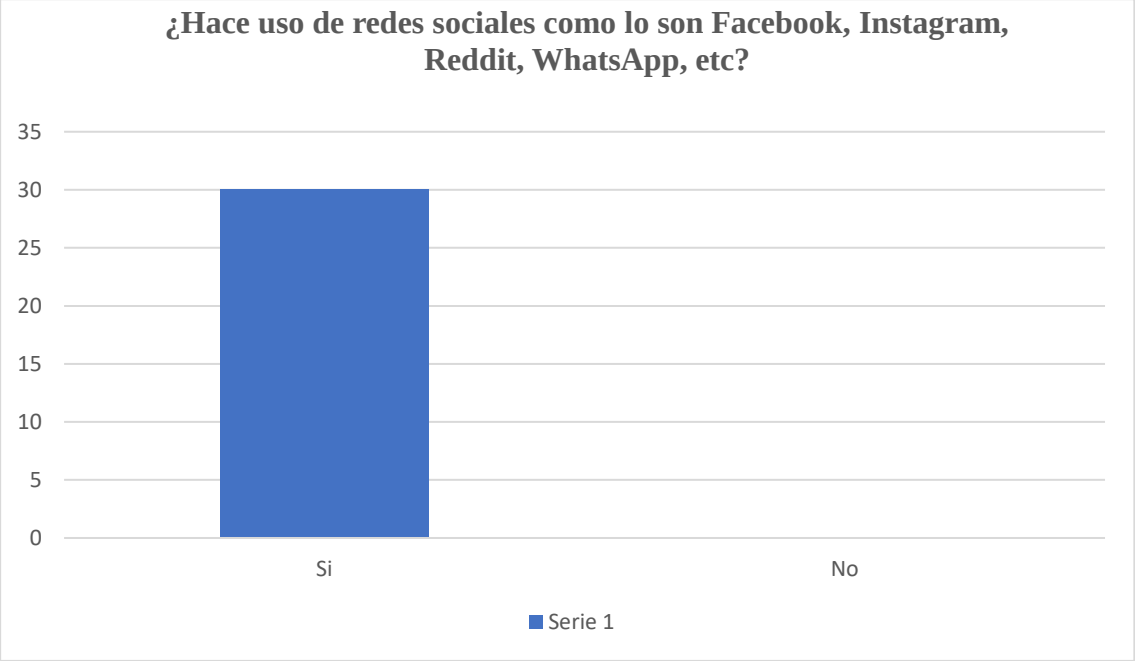
actuales dando asi una imagen de un Estado le falle a su poblacion es su educacion e informacion antes sus nuevos peligros.

Segunda pregunta

¿Hace uso de redes sociales como lo son Facebook, Instagram, Reddit, WhatsApp, etc?

Tabla estadística #2

Figura 2 Uso de redes sociales



Fuente: Sector estudiantil de la ciudad de Loja.

Autor: Miguel Angel Benitez Guayllas.

INDICADORES	VARIABLES	PORCENTAJES
SI	30	100%
NO	0	0%
TOTAL	30	100%

Tabla 2 Uso de redes sociales.

Interpretación

Dado que 30 personas respondieron que si lo cual equivale al 100% de lo encuestados, y basándome en sus respuestas del porqué de la creación de sus cuentas dentro del tema de las redes sociales que si bien no son importantes, pero si indispensables en esta nueva era digital la mayoría de gente responde a la necedad de creación y a su vez el uso para la diversión dentro de las mismas a su vez un grupo delimitado de gente respondió que la usan para la divulgación de su trabajo como lo era el arte, si bien con esto quiero llegar que el uso de las redes sociales y por ende la exposición con el mundo digital es un hecho que no se puede evitar.

Por su otra parte los que respondieron no fueron 0 personas lo cual equivale a un 0%, por lo que podemos decir que toda persona joven cuenta con una cuenta en redes sociales.

Análisis

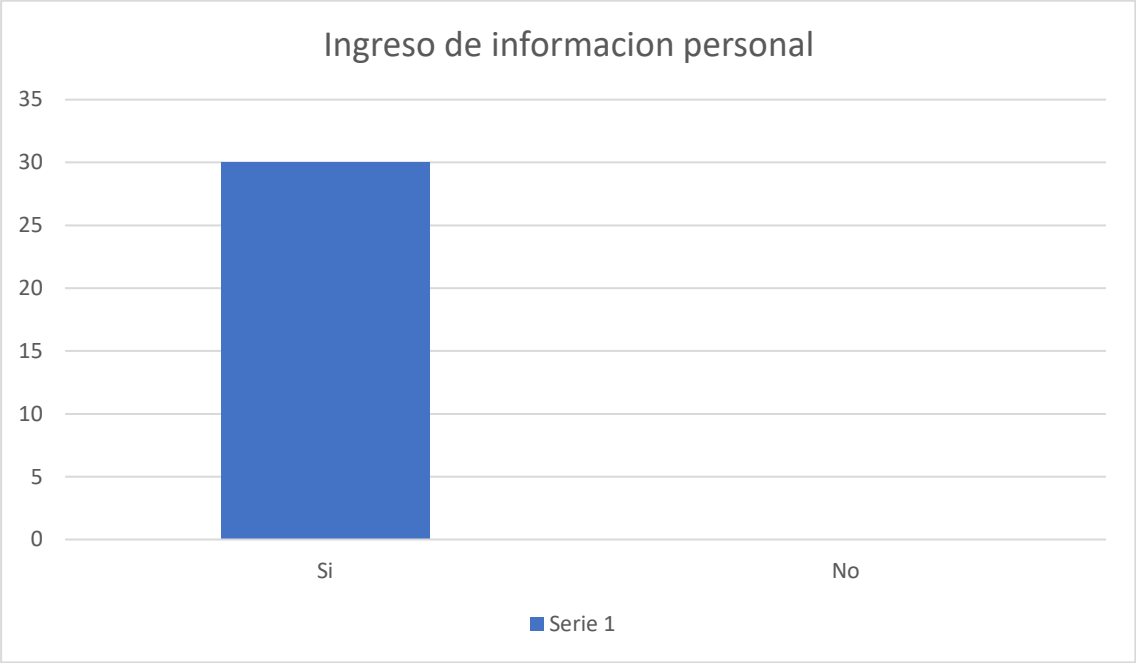
Dado que la mayoría de personas cuentan con alguna red social sea por la razón que sea, decimos que estamos de acuerdo con las opiniones vertidas con los que si cuentan con una red social ya que, en la actualidad la mayoría de personas cuenta con una conexión a internet y citando que en la legislación ecuatoriana, según el artículo 16 de la Constitución de la Republica del Ecuador, en el capítulo segundo, de los derechos del buen vivir, en su sección tercera de comunicación e información sus numerales 2 y 3 estipula: "2. El acceso universal a las tecnologías de información y comunicación. 3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas." (Constitución de la Republica del Ecuador, 2008, pág. 12) con lo anteriormente citado decimos que el derecho a la comunicación y por ende el uso de las redes sociales es un derecho funamental ya que permite a las personas participar plenamente en la sociedad digital lo cual les brinda la oportunidad de desarrollar nuevos cnocimientos, habilidades y oportunidades, pero si bien las redes sociales han sido una opccion de comunicación muy importante en la erea digital tambien asido un nuevo portal para el desarrollo de delitos y una nueva forma de derecho penal

Tercera pregunta

Dado el uso que usted maneja en el internet ¿A ingresado información personal en cualquier página o red social como son nombres, fotos, números de teléfono, correos, etc.?

Figura 3 Ingreso de información personal en páginas o redes sociales

Interpretación



Fuente: Sector estudiantil de la ciudad de Loja.

Autor: Miguel Angel Benitez Guayllas.

INDICADORES	VARIABLES	PORCENTAJES
SI	30	100%
NO	0	0%
TOTAL	30	100%

Tabla 3 Ingreso de información personal en páginas o redes sociales

Interpretación

30 personas, lo cual equivale al 100%, han contestado que han ingresado información personal dentro del internet, o bien para la creación de sus redes sociales, pero a su vez las respuestas han sido variadas unas personas han dicho que han ingresado información como lo es su nombre, correo y fotos. Talvez suene algo insignificante pero los problemas de subir información personal como son los problemas en la privacidad, reputación y seguridad, y esto

también fue pregunta fundamental para dar peso al fundamento de lo que es una persona digital. Pero ¿cuál es el fundamento de la mayoría de las personas para ingresar dicha información? Las 30 personas encuestadas han dado información de que la necedad de ingresar información fue que las propias aplicaciones y webs las requerían para poder dar uso a la misma, entonces talvez estemos hablando de la fragilidad y la facilidad de adquirir información sin ningún tipo de necesidad de exponerse por ello considero un problema actual.

Por su contraparte 0 personas encuestadas, lo cual equivale al 0%, no han ingresado información personal, pero esto solo nos dice cada día las redes sociales son una vía de comunicación necesaria y que cada día se vuelve más mundial y dado que cada vez la información se agrega en el ciberespacio la facilidad que tiene el ciberdelincuente de interferir a la vida cotidiana de una persona es cada vez más fácil es necesario una regularización o una cooperación para que el ciberespacio sea más seguro.

Análisis

Estoy de acuerdo a las opiniones vertidas de los que contestaron de la necesidad de ingresar datos personales dentro de las redes sociales, si bien el cumulo de información como lo es los nombres, las fotos correos, dirección es un concepto fundamental que tiene el ciberdelincuente en acceder a información personal de la víctima decimos que aquí se da lo que es el grado de superioridad del Stalker frente a la persona acosada, dando así paso al concepto de lo que es una persona digital, que como antes señale es "…La persona digital es un modelo de la personalidad publica de un individuo, basado en los datos y mantenido por las transacciones y que ha sido concebido para ser utilizado en representación del individuo…" (VALLEJO, 2010, pág. 14) esto explicado o clarificado en la presente encuesta, las personas encuestadas al momento de ingresar sus datos personales dan inicio a lo que es la creación de su persona digital o como lo verán los otros cibernautas.

Concluimos que, si bien la información personal ingresada al ciberespacio en webs como lo son Facebook, Instagram, etc. Las mismas que son ingresadas bajo el pretexto de una gran mayoría como un requisito para la creación de un perfil ósea el uso de la página social en sí, pero estas páginas ¿para que usan la información? Muy sencillo las mayorías de páginas de redes sociales no te cobran por su uso, entonces ¿cómo pueden mantenerse? El mantenimiento de una red social se basa en el uso de datos personales que los se basan en:

Publicidad: Las redes sociales venden espacio publicitario a empresas que desean promocionar sus productos o servicios. Esto puede incluir anuncios en la plataforma, como anuncios de Facebook o anuncios de Instagram.

Datos: Las redes sociales recopilan y analizan datos sobre sus usuarios para crear perfiles detallados y ofrecer publicidad personalizada. Estos datos también pueden venderse a terceros.

Decimos que si bien, las redes sociables no te cobran, pero estos pueden hacer uso de tus datos, como digo anteriormente, pero a su vez estos datos son vendidos por hackers según el portal Privaci Affairs dado así que en el año 2021 en un foro de hackers se dio venta a datos personales de 500 millones de usuarios de Facebook, con esto quiero decir que los datos subidos a la red son información importante que las personas con conocimiento en el tema de informática o los ciberdelincuentes pueden hacer uso del mismo.

Cuarta pregunta

¿Ha tenido conocimiento o ha sido víctima de un acoso dentro de las redes sociales, como es mensajes de desconocidos, extraños o conocidos revisando constantemente su perfil e incluso recibir mensajes en cualquier medio de comunicación electrónica (Mensajes de WhatsApp, e-mails) de manera constante y por lo cual ha sufrido molestia o miedo?

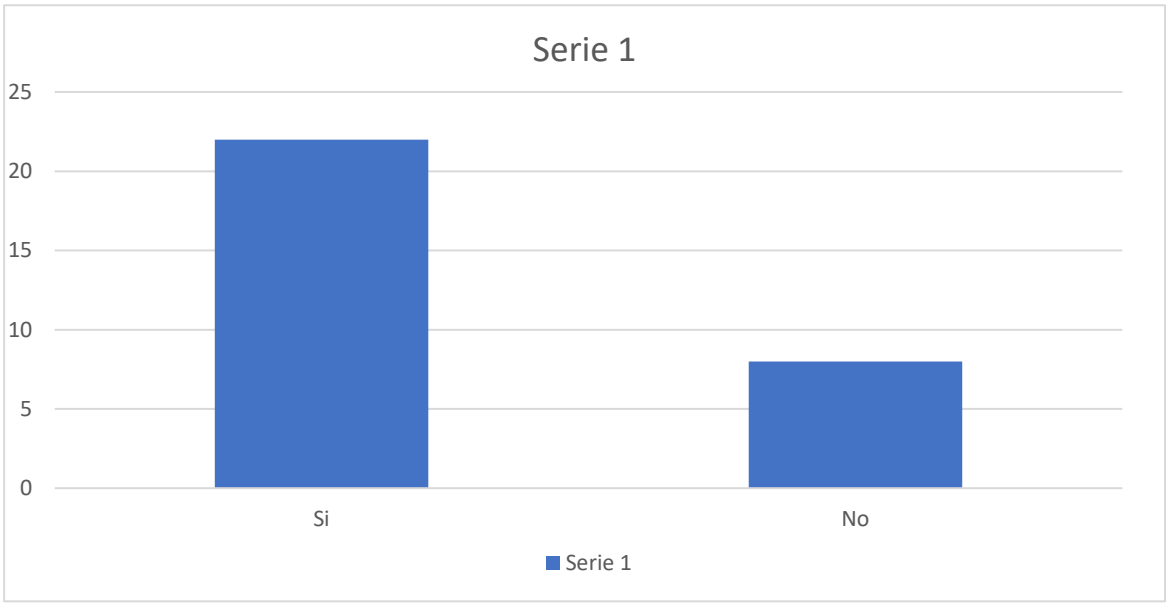


Figura 4 Conocimiento o víctima de un acoso dentro de redes sociales

Fuente: Sector estudiantil de la ciudad de Loja.

Autor: Miguel Angel Benitez Guayllas.

INDICADORES	VARIABLES	PORCENTAJES
SI	22	73.3%
NO	8	26.7%
TOTAL	30	100%

Tabla 4 Conocimiento o víctima de un acoso dentro de redes sociales

Interpretación

22 personas que es equivalente al 73.3% de los encuestados, marcaron que han recibido mensajes de extraños, los mismos que les han resultado molestos e incluso algunos les ha provocado miedo al momento de recibirlos, pero el factor más interesante al analizar es que la mayoría de personas encuestadas que respondieron si a esta pregunta fueron mujeres, entonces se entiende que estos problemas afectan principalmente a mujeres las mismas que supieron manifestar que la mayoría de mensajes recibidos correspondían a extraños o de perfiles falsos los mismos que llevan al anonimato.

8 personas que es equivalente al 26.7% de los encuestados, han contestado que no han recibido mensajes de este tipo, pero en su mayoría son encuestas llenadas por hombres y esto solo ratifica que esta nueva figura delictiva afecta más a mujeres, que si bien la mayoría del porque fue en su generalidad que estos no son receptores de estos tipos de mensajes.

Análisis

Decimos que con la información recolectada se constata que existe un patrón de conducta, una conducta dirigida repetitivamente contra un individuo concreto que este experimente como intrusiva o no deseada y que le cause miedo o intimidación, dando así una de las características del ciberstalking, con esto en mente, podemos decir que la mayoría de víctimas o sujetos pasivos son relacionadas al sexo que es el femenino y sus autores o sujetos activos son en su mayoría de sexo masculino.

Como sabemos las características del ciberstalking cumple una serie de características y bajo esta pregunta se cubren los algunos puntos antes ya mencionados en el marco teórico, en esta pregunta se abarca la característica de;

La situación de poder en la que se encuentra el acosador, gracias a ese anonimato del que goza, y que pueda utilizar tanto respecto de personas que ya conoce, como de aquellas a las que conoce a través de chats o foros de la más variada naturaleza: En la presente encuesta, los encuestados responden que la gente que les escribe por redes son gente que no conoce y en otros casos con perfiles falsos, entonces llegamos a la conclusión que en perfiles falsos la información proporcionada en dicha cuenta es falsa, por ende no se sabe quién llegando a un estado de indefensión provocado por el anonimato que da este medio.

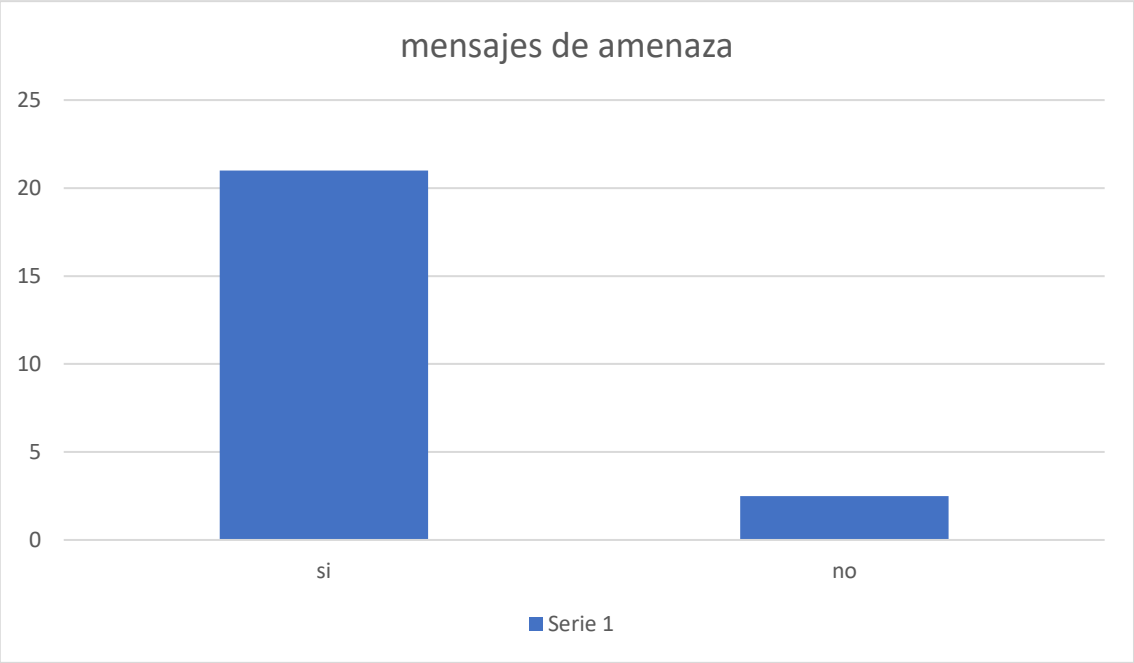
La importante información que puede recibir el acosador de la propia víctima a través de sus perfiles, información que puede referirse a su vida personal o privada y que resulte fundamental para el Stalker: Con las encuestas se verifico que el Stalker (Sujeto activo) se ayuda de la información personal que es facilitada por las redes sociales, basándose su idea y concepto de la persona desde la persona virtual que no es más que la representación de la persona natural en la virtualidad.

Concluimos que, la principal conducta que presenta el sujeto activo es la actitud del acoso dentro de redes sociales, mismo que hace uso de la información proporcionada por la red, exigía una conducta dirigida repetitivamente contra un individuo concreto (Sujeto pasivo) que este experimente como intrusiva o no deseada y que le cause miedo o intimidación dando así una violación y a un bien tutelado como es la intimidad.

Quinta pregunta

¿Ha recibido algún tipo de amenaza, difamación, humillación, acoso sexual, invasión de la privacidad u otros comportamientos abusivos o agresivos?

Figura 5 Recibir amenazas, difamación, humillación, acoso sexual, invasión de privacidad u otros comportamientos abusivos.



Fuente: Sector estudiantil de la ciudad de Loja.

Autor: Miguel Angel Benitez Guayllas.

INDICADORES	VARIABLES	PORCENTAJES
SI	21	70%
NO	9	30%
TOTAL	30	100%

Tabla 5 Recibir amenazas, difamación, humillación, acoso sexual, invasión de privacidad u otros comportamientos abusivos.

Interpretación

21 personas encuestadas equivalentes al 70%, han respondido que si han recibido un mensaje de amenaza, pero, dentro del mismo en su respuesta han insertado unas actividades algunas con susceptibilidad de análisis, como lo es la modificación de fotos pre subidas con la finalidad de amenazar a la persona que se está tratando de mantener un vínculo, sea o no conocida, con esto se demuestra que dentro de la población estudiantil dentro del rango de 16-17 años sufren de acoso en las redes dando así un impunidad del sujeto activo (Stalker).dando así protegido dignidad e integridad personal derechos protegidos en la constitución, con esto digo que si bien

estos bienes jurídicos están protegidos, en la actualidad en la virtualidad estos son vulnerados sin ningún tipo de castigo.

Por su otra parte, 9 personas que son equivalentes al 30% de los encuestados nos señalan que no han recibido este tipo de comportamientos, algunos de ellos nos señalan que tienen desactivado los mensajes de extraños y otros directamente nunca han recibido estos, pero si bien se me hace factible señalar que la mayoría de esta respuesta fue dada por el género masculino el mismo que si bien también es afectado, pero en una menor medida que el género femenino.

Análisis

Estoy de acuerdo con las opiniones vertidas por la mayoría, ya que la característica del ciberstalking es hacer sentir incomodidad a la víctima, dado que las mismas reciben mensajes amenazantes y algunas veces difamatorios ya que hacen uso de sus fotos que han subido a las redes sociales haciendo uso de una herramienta de Photoshop para poner en usa situación de indefensión a la víctima (sujeto pasivo) en este punto se cumplen el resto de características de esta nueva modalidad de stalking que son:

La situación de poder en la que se encuentra el acosador, gracias a ese anonimato del que goza, y que pueda utilizar tanto respecto de personas que ya conoce, como de aquellas a las que conoce a través de chats o foros de la más variada naturaleza: La situación de poder frente a la víctima se da en el momento que es capaz de contactar a otra persona, enviar un mensaje y tener la capacidad de manipular sus datos como lo son sus fotos dando así una situación de indefensión.

El problema radica en la distancia y a veces en la falta de capacidad o nula información del sujeto activo (Stalker) esto se da que estos delitos son realizados mediante el ciberespacio lo cual lo realizan en la privacidad de sus casas y en otros casos en sujetos más expertos dentro de una computadora que tenga los programas necesarios para ocultar tanto su ubicación como datos relacionados dando así que aumente su relación de poder

La circunstancia de que es la propia red la que proporciona los diferentes medios que utiliza el stalker. Sirva como ejemplo el envío de mensajes online, de contenido variado (insultante, amenazante) y de cadencia variable, sistemática o masiva (mail bombing). Dichos envíos de e-mail pueden ser de carácter anónimo, a través de e-mail gratuito, por ejemplo, o manipulados para que parezcan enviados por la propia víctima, lo que puede

colocarla en muy difícil situación: El problema central de las redes sociales, es la facilidad de sacar información de una persona (Persona digital) todo lo que sea subido a la red, aunque lo borres nunca dejara de existir en la red, entonces decimos que existen dos características de la red que los stalkers usan para realizar estos actos que son:

1. Los datos que dejamos en internet son imborrables.
2. Todo lo que se sube a internet deja de ser privado y se vuelve publico

La posibilidad de manipular fotografías o imágenes de la víctima que se encuentren en Internet y que hayan sido facilitadas por ella misma en alguna de sus redes sociales o chats. Otra posibilidad puede ser colgar contenidos ofensivos dedicados a la víctima o utilizar servicios de mensajes (sms) desde la red, pues no pueden identificarse fácilmente: Como recalcamos en el anterior punto todo lo subido al internet deja de ser privado y se vuelve público, con esto decimos que si bien las fotos son de la persona que la posteo no cabe duda que cualquier persona puede hacer uso de la misma e inclusive modificarla como es el ejemplo de realizar un montaje de la cara de la persona en un cuerpo desnudo dando así que parezca que la persona que subió dicha foto sea la misma de esa imagen.

Con esto el Stalker le envía las fotos a la víctima dando así una humillación y invasión a la privacidad dentro de la virtualidad,

6.2.Entrevistas

1. El derecho de la comunicación y la información se encuentra en la C.R.E. en el artículo 16 en sus numerales 1 y 2 que estipula: **1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos 2. El acceso universal a las tecnologías de información y comunicación. ¿Cree usted que el de acceso a estas redes debería ser controlado ya sea por el fiscal o la policía cibernética con la finalidad de prevenir la impunidad de los ciberdelincuentes?**

Primer entrevistado

Si bien es cierto la constitución establece la libertad para poder comunicarnos, es interesante que todo derecho tiene limitación, la constitución nos da una amplitud de derechos sin embargo hay normas de menor jerarquía o supra e infra constitucionales que modulan la constitución, y es necesario establecer en normas de menor jerarquía el control porque si no daríamos rienda suelta de inmiscuirse muchos tipos de delitos incluso en lo que ahora se da bastante en delitos

como: delitos sexuales, crimen organizado tiene mucho que ver la virtualidad, entonces si es necesario ejercer el control sobre todo, y sobre todo en los menores de edad que no tienen el control suficiente para saber hacia dónde se están orientando, entonces si es necesario un control y tener una especie de filtros que permita sistematizar la información

Segundo Entrevistado

El acceso como tal es un fenómeno difícil de controlar en razón de la universalidad de la problemática, sin embargo si se aterriza esa problemática en los fenómenos criminales concretos o en casos concretos el acceso a la misma y el tratamiento a la misma si podría y si debería ser controlado por parte de las autoridades pertinentes, no así todo acceso a las tecnologías de la información y comunicación en razón a la universalidad del problema, es demasiado bien jurídico para tutelar, primero debería partir de una responsabilidad individual en relación a la prevención de parte de los padres o tutores luego de las autoridades e instituciones para finalmente la persecución de los casos concretos que ya convertidas en figuras delictivas si ser tratadas de parte del estado

Tercer entrevistado

En primer lugar, está determinado, el hecho del acceso a las tecnologías de la información y la comunicación de todo ciudadano, ahora bien, el control prácticamente de esto se viene determinando desde la secretaria de telecomunicaciones tratándose las TIC, si se quiere involucrar a la policía o el fiscal pues se trataría en casos concretos en el evento en que se cometan conductas penalmente relevantes

Cuarto entrevistado

Como una medida para prevenir la impunidad de los ciberdelincuentes. Esta es una cuestión compleja y debe analizarse cuidadosamente para determinar si es una solución adecuada y efectiva. En primer lugar, es importante tener en cuenta que la privacidad y la libertad en línea son derechos fundamentales que deben ser protegidos. La implementación de medidas para controlar el acceso a las redes puede ser vista como una restricción a estas libertades, por lo que es necesario encontrar un equilibrio entre la seguridad y la privacidad.

También es importante considerar que el control del acceso a las redes no necesariamente garantiza la prevención de la impunidad de los ciberdelincuentes. A menudo, los ciberdelincuentes utilizan técnicas avanzadas para ocultar su identidad y rastros digitales, lo que hace que sea difícil rastrearlos y procesarlos legalmente.

Quinto entrevistado

El control del acceso a las redes por parte de la policía cibernética o el fiscal podría ser una medida necesaria para prevenir la impunidad de los ciberdelincuentes. En este sentido, se podría argumentar que la privacidad y la libertad en línea deben ser equilibradas con la necesidad de proteger a los ciudadanos de los delitos en línea ya que los ciberdelitos son una amenaza cada vez mayor, y el aumento de la actividad criminal en línea puede tener graves consecuencias para los individuos, las empresas y las sociedades en general. Por lo tanto, la implementación de medidas para controlar el acceso a las redes podría ser vista como una herramienta efectiva para prevenir y perseguir estos delitos.

Además, se podría argumentar que el control del acceso a las redes podría ser una medida temporal y específica, utilizada solo para fines de investigación y persecución de delitos graves. Esto significaría que la privacidad y la libertad en línea no estarían permanentemente restringidas y que solo se tomarían medidas cuando fuera necesario.

Comentarios del autor:

Comparto con las opiniones vertidas con los entrevistados, dando así que la importancia del control dentro de las redes sociales es indispensable para el control del ciberdelincuente y por ende su sanción, pero a su vez respetando el derecho básico que tiene todo ciudadano a su privacidad ya que solo se intervendrá a su control en casos muy concretos tal es el caso como si fuera sospechoso de cometer algún delito. Dando así una verdadera persecución del enemigo mismo que lo señalamos en el marco teórico el cual abarca 3 puntos fundamentales los mismos que son **1.- Adelanta la punición de determinadas conductas aun antes de que se consuma la ejecución de las mismas:** Esto se cumple dado el adelanto en la prevención dado el control preventivo del medio en que se cometen estas nuevas figuras delictivas.**2.- Castiga determinadas conductas que no se han hecho con la misma penalidad que si se hubiese realizado:** Si bien la revisión y control ayuda a precautelar la finalidad de la figura delictiva en este apartado se puede castigar los pasos para llegar a consumar la misma.**3.- Se establece una serie de medidas que reducen garantías individuales:** Dado que al momento de dar un control se limita los derechos de libertad y privacidad es un mal necesario para proteger un bien jurídico mayor,

2.- La falta de tipificación de esta figura en el derecho penal, ha llevado a una impunidad por no estar sujeta a una sanción que es el objetivo de la norma ¿Cree usted que es necesaria la tipificación de esta figura delictiva?

Primer entrevistado

Todo lo que tiene que ver con la protección de bienes jurídicos es necesario, lo que abunda son los delitos cometidos en redes informáticas entonces es necesario modernizarse, estamos en una época de la globalización y es necesario que partiendo de los principios de legalidad y reserva se pueda establecer la tipificación de los delitos para evitar en lo posible, porque realmente establecer en la norma no nos deja impunes, pero si nos previene.

Segundo Entrevistado

Sin ninguna duda, ante la aparición de nuevas figuras delictivas, sobre todo, con el aparecimiento y la modernización de las tecnologías de la comunicación tipificar nuevas figuras que tengan que ver con los ciberdelitos y demás cada día es más necesaria la tipificación en las legislaciones mundiales, es un tema que seguramente en la legislación nacional tiene un algo de retraso pero a de tipificarse en la razón de la necesidad que tiene en el mundo moderno

Tercer entrevistado

Definitivamente, no hay ningún problema sería conveniente la tipificación y sanción en el catálogo delitos en el COIP a efecto de que se pueda sancionar esta conducta y ya lo tenemos claro que hay conductas que en algunos casos no se han dejado de sancionar sin embargo hay casos que por la complejidad como que se nos da la idea que queda en la impunidad, no estaría mal que se tipifique y sancione como una conducta independiente

Cuarto entrevistado

Sí, es necesaria la tipificación de la figura del ciberstalking en el derecho penal para combatir eficazmente este delito y prevenir la impunidad de los perpetradores. El ciberstalking es una forma de acoso en línea que puede tener graves consecuencias para las víctimas, como ansiedad, depresión, estrés postraumático e incluso suicidio. Es por ello que la tipificación de esta figura delictiva es esencial para proteger a las personas que pueden ser víctimas de este tipo de acoso. Y también permitiría a las autoridades actuar con mayor rapidez y eficacia para investigar y procesar a los perpetradores

Quinto entrevistado

El ciberstalking es una forma particularmente insidiosa de acoso que puede tener efectos devastadores en las víctimas y que merece una respuesta legal específica. El ciberstalking no se limita a un solo acto de acoso, sino que es un patrón persistente de comportamiento hostil y

amenazador que puede tener un impacto duradero en la salud mental y emocional de la víctima. A menudo es difícil de probar en un tribunal debido a la naturaleza intangible de la evidencia en línea, lo que hace que sea aún más importante tener leyes claras y específicas para proteger a las víctimas y castigar a los perpetradores.

La tipificación del ciberstalking en el derecho penal permitiría a los tribunales procesar a los acosadores por su comportamiento específico y tomar medidas legales para detenerlo. También puede ayudar a prevenir futuros actos de acoso en línea, ya que la clara definición del delito y la penalización asociada pueden disuadir a los posibles acosadores de cometer este tipo de actos.

Comentario del autor:

Estoy de acuerdo con las opiniones dadas por los encuestados, básicamente concuerdan con mi opinión de la necesidad de tipificar esta nueva figura delictiva, pero en su mayoría nos dieron dos características que es menester manifestar:

_La necesidad de tipificación de esta nueva conducta como base de diferenciación de otras conductas relacionadas: con esto nos referimos a la importancia de definir y clasificar una nueva conducta específica en relación con otras conductas similares, con el fin de distinguirla y entenderla mejo adecuando el problema que representa y a su vez establecer un marco legal y que permita su prevención.

_ La necesidad de tipificación como base de prevención: Nos referimos a la idea de que la definición clara y precisa de una conducta específica, a través de su tipificación en la ley, puede ser una herramienta importante en la prevención de esa conducta ya que cuando una conducta está tipificada, es decir, definida de manera clara y precisa en el marco legal, se puede aumentar la conciencia pública sobre ella y se pueden establecer medidas preventivas específicas para evitar que se produzcan casos de esa conducta. Además, una vez que la conducta ha sido tipificada, las autoridades tienen más herramientas para investigar y castigar a quienes la cometan.

3.-El anonimato es uno de los principales problemas al momento de identificar al sujeto activo y por ende su sanción, ¿Se debería dar la potestad al fiscal para que pueda acceder a los dispositivos electrónicos de una persona si esta es sospechosa de cometer algún tipo de delito?

Primer entrevistado

Dentro del Código Orgánico Integral Penal si dispone la apertura de los celulares, entra a una cadena de custodia pero realmente como una normativa existe como una técnica de investigación, actualmente se hace la apertura porque tiene que entrar como evidencia cuando se ha cometido un hecho punible para poder esclarecer como producto de la infracción, los celulares en este tipo de delitos es fundamental ya que constituye los vestigios por el cual se cometió el delito entonces si nos da la facultad de que el fiscal pueda apertura, pero si se le puede dar un alcance mas amplio o describir aspectos que no estén concretados se los podría hacer con la finalidad de esclarecer el hecho punible.

Segundo Entrevistado

Si nos referimos a una persona que sospechosa dentro del proceso penal ya está fijada dentro de la fase preparatoria del proceso penal, esa potestad es parte de los fiscales, sin embargo, si se trata de perseguir esa figura desde la prevención si considero que se debería liberar el acceso a esta información, para que pueda derivara la captura o persecución del delito para que la información no sea eliminada por los ciberdelincuentes

Tercer entrevistado

Si hay la posibilidad que en un proceso penal, la investigación sea en la preprocesal o procesal tiene la posibilidad de que el fiscal disponer algunas diligencias apoyándose del sistema penal de medicina legal y ciencia forense definitivamente si tiene la posibilidad de poder determinar elementos suficientes en primer lugar establecer una conducta penal legalmente relevante y responsabilidad de una persona que una persona pueda ser sospechosa, entonces en este sentido si tiene la posibilidad el fiscal.

Cuarto entrevistado

El COIP tiene en su normativa el sustento legal para la correcta revisión, pero este es dentro del proceso, pero si nos referimos en algo fuera de un proceso y que sea como medida preventiva la cuestión del acceso a los dispositivos electrónicos de una persona sospechosa de cometer un delito es un tema muy complejo y delicado. Si bien el anonimato en línea puede dificultar la identificación de los autores de ciertos delitos, el acceso indiscriminado a los dispositivos electrónicos de las personas podría plantear problemas graves de privacidad y de derechos civiles. En cuanto a la potestad del fiscal para acceder a los dispositivos electrónicos, esto también puede ser problemático si no se establecen salvaguardas adecuadas. Si bien es importante que las autoridades puedan investigar y castigar los delitos en línea, es igualmente

importante garantizar que se respeten los derechos y libertades de las personas y se evite el abuso de poder.

Quinto entrevistado

En un proceso penal que tenga como medio la utilización los medios electrónicos o el uso de las TIC se pide como prueba fundamental el dispositivo mediante el cual se realizaron estos actos, entonces decimos que se encuentra como tal normado en nuestro procedimiento penal, pero esto llevado a un proceso fuera o de carácter anticipado a llegar a un proceso el acceso a los dispositivos electrónicos de una persona sospechosa de cometer un delito es un tema delicado que debe ser objeto de debate cuidadoso y considerado, y estar sujeto a salvaguardas legales adecuadas para proteger los derechos y las libertades de las personas.

Comentario del autor:

Si bien la base legal de la revisión de dispositivos electrónicos esta en el procedimiento penal el mismo señalado en el Código Orgánico Integral Penal, dando así una normativa de vigilancia y análisis pero esto dentro del proceso, mi relevancia de la pregunta se centra en la revisión de los dispositivos antes de que ocurra el hecho dando así una medida de prevención a esta nueva modalidad.

4.- La figura denominada ciberstalking se la comete por medio del internet utilizando redes sociales o cualquier medio que se use para conectar a más cibernautas, por ende, este no es un problema nacional, ya que el Internet es a nivel mundial, según su criterio ¿Para controlar el comportamiento del ciberdelincuente, y por ende sea susceptible a una sanción o pena, se necesite la cooperación internacional?

Primer entrevistado

Es necesario la cooperación internacional, lo que pasa es que el crimen organizado sobredimensiona las fronteras nacionales, las latitudes geográficas se ven limitadas entonces se necesita la cooperación internacional y con eso se lograría una cooperación eficaz y trabajar mutuamente frente a estas figuras nuevas pero que son parte del crimen organizado, entonces yo pienso que es una forma de poder actuar y cerrar las brechas al crimen.

Segundo Entrevistado

Todos los ciberdelitos que están tipificados y los que han de tipificarse tienen que er tratados como los delitos de carácter transnacional en razón de la variedad de sujetos activos que pueden

caber en esta figura delictiva, la concurrencia respecto a las tecnologías que también pueden encontrarse fuera del ámbito territorial de protección del código orgánico integral penal y del estado ecuatoriano entonces esas figuran si merecen y si deberían tratarse como delitos transnacionales con cooperación internacional

Tercer entrevistado

Indudablemente al tratarse de conductas que trascienden las fronteras es importante la cooperación y de hecho con sus similares cuando investiga el fiscal ahí si abrí que reflexionar en el sentido si es que le dedica el tiempo suficiente para investigar este delito o simple y llanamente el fiscal deja transcurrir el tiempo y a lo mejor archivarlo entonces esa cuestión es la que tenemos que analizar es decir que hay el compromiso del fiscal de investigar esos hechos.

Cuarto entrevistado

Si bien es cierto que el ciberstalking es un problema global que se puede cometer desde cualquier lugar del mundo y que afecta a víctimas en todo el mundo. Debido a esto, para controlar el comportamiento del ciberdelincuente y hacer que sea susceptible a una sanción o pena, a menudo se necesita la cooperación internacional.

Los ciberdelincuentes pueden ocultar su identidad y ubicación física utilizando diversas técnicas de anonimización en línea, lo que dificulta la identificación y el enjuiciamiento de los perpetradores. Además, la naturaleza global de Internet significa que los delitos cometidos en línea pueden cruzar las fronteras nacionales y jurisdicciones legales, lo que complica aún más la aplicación de la ley, la cooperación internacional entre las agencias encargadas de hacer cumplir la ley en diferentes países es esencial para abordar el ciberstalking y otros delitos en línea.

Quinto entrevistado

Sí es necesario, el ciberstalking es un problema que puede trascender las fronteras nacionales debido a que las acciones del delincuente pueden afectar a personas en diferentes países. Para combatir este delito, es importante contar con la cooperación internacional de las autoridades encargadas de hacer cumplir la ley.

En muchos casos, el ciber Stalker puede ocultar su identidad o ubicación a través del uso de tecnologías avanzadas, lo que hace que sea difícil para las autoridades locales rastrearlos y detenerlos. Por esta razón, se necesita la cooperación entre diferentes agencias de aplicación de

la ley en todo el mundo para compartir información, investigar y perseguir a los ciberdelincuentes.

Comentario de autor:

Estoy de acuerdo con las opiniones recopiladas, si bien en el marco teórico he señalado la indispensable y necesaria cooperación internacional como medida tanto de prevención como de identificación y persecución del ciberdelincuente se necesita de tres fases detalladas anteriormente que son la Cooperación, asimilación y armonización unificación normativa las mismas que son concetos abordados en su totalidad como forma lucha contra estas figuras delictivas que usan como medio de sus actividades delictivas.

5.- El sujeto pasivo, la victima de esta figura delictiva del ciberstalking sufre daño moral, psicología e incluso daño físico, y por consecuencia la reparación integral son gastos que son pagados por la víctima, Según su criterio ¿El estado debería proporcionar el tratamiento gratuito a la víctima?

Primer entrevistado

Ahora el código orgánico integral penal, como medida de reparación debe asumir la responsabilidad el sujeto activo como lo establece el Art 78 de COIP sin embargo el estado debería establecer políticas de acción, estableciendo grupos estratégicos y ´políticas de prevención, para que no se vuelva a reincidir en la comisión del delito entonces podríamos hablar de la construcción social de entidades encargar de prevenir, reprimir y sancionar entonces desde esa perspectiva si podríamos considerarlo como aquellas instituciones o instrumentos que permitan hacer un control eficaz encaminado en el control social punitivo de la criminalidad, entonces ahí si podríamos establecer instituciones que asuman un rol, no delegando la función directamente al estado pero asumiendo la función que tiene el estado como un protector y benefactor de los derechos de las personas y como quien ejerce el control punitivo de la criminalidad entonces en ese sentido si delegaríamos la responsabilidad social de reparar a la víctimas en el tratamiento psicológico pero no independientemente sino solidariamente, e incluso analizando la posibilidad de quienes tienen la economía para poder subsidiarse los gastos.

Segundo Entrevistado

Yo creo que, el estado si debería proporcionar tratamiento a la víctima pero no gratuito, me parece que hay una gran tarea para todas las autoridades respecto a que se incluya dentro de las

reparaciones integrales los costos de los tratamientos incurridos por parte de la víctima para que estos sean pagados por la persona que termina siendo determinada como sujeto activo de los delitos en virtud de que el estado ya proporciona tratamiento de las victimas pero estos deberían ser proporcionados en su totalidad por los sujetos activos.

Tercer entrevistado

En primer lugar, lo que se determina la reparación integral del sujeto activo de la infracción sin embargo no está por demás que el estado contribuya y aporta y se preocupe definitivamente en que esa persona sea reparada íntegramente tratándose de cuestiones de salud.

Cuarto entrevistado

Sí, el estado debería proporcionar tratamiento gratuito a las víctimas de ciberstalking que han sufrido daño moral, psicológico y/o físico como consecuencia del delito. Las víctimas de ciberstalking a menudo sufren una gran cantidad de daño emocional, que puede requerir asistencia psicológica o psiquiátrica para su recuperación. También pueden necesitar tratamiento médico si han sido víctimas de acoso físico.

Es responsabilidad del estado garantizar la protección y el bienestar de sus ciudadanos, y esto incluye proteger a las víctimas de delitos cibernéticos y ayudarlas a recuperarse de los daños causados por los mismos.

Quinto entrevistado

Desde una perspectiva ética y moral, es responsabilidad del estado garantizar el bienestar de sus ciudadanos y protegerlos de los delitos, incluyendo el ciberstalking. Por lo tanto, el estado debería proporcionar asistencia y tratamiento gratuito a las víctimas de ciberstalking para ayudarles a recuperarse del daño sufrido, además, proporcionar tratamiento gratuito a las víctimas de ciberstalking no solo es importante para ayudar a las víctimas a superar el trauma, sino que también es una forma de prevenir la repetición del delito

Comentario del autor

Compartiendo con las opiniones antes descritas, diré que la responsabilidad que tiene el estado como un ente protector y que garantiza al derecho bienes jurídicos enmarcados en su constitución, estos al momento de ser violentados y no ser restituidos por el motivo de que esta figura no es tipificada y por ende una de las finalidades del derecho penal que es la reparación integral no se logra, el estado debería apoyar no en su totalidad pero si en parte en su proceso

de recuperación por que el sujeto activo como debería ser en un procedimiento ordinario debería encargarse de pagar los gastos, pero como no se encuentra tipificado en el COIP los gatos son proporcionados por la victima dando así un afecto directo al patrimonio individual por un daño que ella no provoco.

6.3.Estudio de casos

Noticia #1

Sacarlett Camberos sufre acoso y hackeo de sus redes sociales

El Club América femenil emitió su postura y condenó la violencia y acoso que ha sufrido su jugadora Scarlett Camberos

#XICO #MA #jugadora #redes #acoso #América Femenil #Instagram #América #Club #Â

CIUDAD DE MÉXICO.- El nombre de **Scarlett Camberos**, jugadora del **América Femenil,** se convirtió en tendencia en las redes sociales, debido a que la jugadora mexicoamericana sufrió de acoso y sus redes sociales fueron hackeadas.

El padre de la futbolista, **Jorge Camberos**, fue quien denunció que su hija de 22 años, había sido víctima de acoso de parte de una persona que aparentemente es su ex pareja.

Jorge Camberos
@JorgeCamberos24 · **Seguir**

Aviso! Las redes sociales de Scarlett fueron hackeadas por el enfermito que la a estado acosando. Por favor no le sigan el rollo y su juego

3:21 a. m. · 14 feb. 2023

1,9 mil **Responder** **Compartir**

Leer 98 respuestas

"¡Aviso! Las redes sociales de Scarlett fueron hackeadas por el enfermito que la ha estado acosando. Por favor no le sigan el rollo y su juego".

A través de la cuenta de Twitter de **Camberos**, se denunció las supuestas agresiones de las que ha sido víctima, sin embargo se desconoce hasta el momento si realmente fue la propia jugadora quien publicó los mensajes o si fueron realizados por la persona que hackeó sus cuentas.

El pasado año del 2022, **Scarlett Camberos** denunció a una persona que creaba cuentas faltas en **Instagram** para acosarla.

"Hola, ocupo su ayuda en reportar esta cuenta por favor. Este muchacho sigue creando cuentas falsas de mí en redes sociales y acosándome. Este es su Instagram, ya no soporto más todas las cuentas que hace para molestarme a diario y hoy me lo topé en mi camino a casa. Acosando NO ESTÁ BIEN", escribió la americanista.

Link de la noticia: Sacarlett Camberos sufre acoso y hackeo de sus redes sociales (posta.com.mx)

Infractor: Desconocido dado el anonimato que presenta las redes sociales, pero se presume que es el exnovio de género masculino. fue el mismo que le enviaba mensajes desde otra cuenta, pero en un perfil falso.

Victima: La victima es la señorita Scarleet Camberos, la cual se evidencia que las principales víctimas son del género femenino.

Hechos: La señorita Scarleet Camberos comenzó a sufrir acoso de su expareja dentro de las redes sociales acosándola, la misma que no le toma más importancia de la normal. Pero el problema surge cuando su expareja desde diferentes perfiles falsos le manda mensajes reiterados los mismos que le causan molestia y miedo. Dando así actitudes que son características del ciberstalking.

Comentarios: Dada la noticia presentada anteriormente se puede destacar lo siguiente:

El presunto agresor fue su expareja, misma que al saber que no respondía sus mensajes intento mediante perfiles creados por el con información falsa, dando así una conducta típica del ciberstalking.

El acoso recibido dentro de sus redes sociales escalo a tal punto que el sujeto pasivo provoco miedo a la víctima, dando así el hackeo de la cuenta y con ello usando su información dio uso de la cuenta enviando mensajes a sus contactos y difamándola.

La manifestación de esta conducta es una situación que en su mayoría queda en la impunidad, ya que en primera no se puede comprobar al sujeto activo dado el anonimato creado en la red solo existe un supuesto al cual no se le puede juzgar dando así una situación de poder que tiene el sujeto activo frente al sujeto activo.

Caso #2

Acoso sexual en redes acecha a los jóvenes en Ecuador

Un padre de familia de un colegio particular de la Zona 8 dio la alerta de acoso sexual. Su hija de 12 años había recibido 100 mensajes de un compañero en los que pedía que le envíe una foto de ella desnuda.. Foto Pixabay

Mario Naranjo, Editor

Un padre de familia de un colegio particular de la Zona 8, compuesta por Guayaquil, Durán y Samborondón, dio la alerta de acoso sexual. Su hija de 12 años había recibido 100 mensajes de un compañero de aula, en todos ellos le pedía que le envíe una foto de ella desnuda mientras se duchaba.

17:11 Operativo de control durante Carnaval en Quito
17:11 Hoteleros de Santa Elena registran reservas del 100% por Carnaval
17:09 Bayer Leverkusen de Piero Hincapié pierde en Europa League
17:04 Moisés Caicedo y Pervis Estupiñán, con más multas en Brighton

VER MÁS

VIDEOS DESTACADOS

1 Juez debe revisar 7 600 fojas en caso María Belén Bernal

Caso inédito de niña con cáncer de mama en Chile sorprende a médicos

Abogados del caso María Belén Bernal presentarán 200 testigos

Link de la noticia: Acoso sexual en redes acecha a los jóvenes en Ecuador - El Comercio

Infractor: Sujeto activo de género masculino, los mismos que fueros identificados como compañero de aula.

Victima: Sujeto pasivo de género femenino, compañera de clase.

Hechos: Un padre de familia de un colegio particular de la Zona 8, compuesta por Guayaquil, Durán y Samborondón, dio la alerta de acoso sexual. Su hija de 12 años había recibido 100 mensajes de un compañero de aula, en todos ellos le pedía que le envíe una foto de ella desnuda mientras se duchaba.

El menor utilizó el servicio de mensajería de una de las redes sociales para hacerlo. Ante el acoso, la menor reportó a sus padres y ellos al colegio.

Pero lo realmente preocupante y que cambio la dirección de la investigación fue que el menor, que acosaba a su compañera, era extorsionado por un adulto a pedir dichas fotos.

Comentario: Dado los hechos expuestos anteriormente se dice que existen varios factores a analizar el primero seria la falta de atención que le prestan los tutores legales a los menores de edad dando así que existan contactos que tiene un menor de edad con otras gentes en juegos virtuales y que los mismos amenacen a estos con la intención de acosar a sus compañeras y con esto llegando a la figura de que la persona mayor que amenazo al mayor se convierta en el autor intelectual de esta figura, y por otro lado la facilidad que tienen las personas de amenazar y

infundir miedo en las redes sociales, las mismas que las victimas por miedo o molestia buscan una salida y ya sea por desconocimiento y falta de madurez obedezcan al Stalker.

Caso #3

Link de noticia: Mamarazzis: Clara Chía, harta de sufrir acoso en las redes sociales (elperiodico.com)

Infractor: Sujeto activo: Grupo de personas las cuales son un número muy grande que acosan Clara Chia, el número es tan grande que es casi imposible identificar a todos.

Victima: Sujeto pasivo de género femenino, Clara chía.

Hechos: la joven de 22 años está encajando el pasar de ser una persona anónima a estar en el centro del foco mediático rosa. Algo que ha ido a más tras la canción de Shakira con Bizarrap, que estaba llena de mensajes envenenados hacia Piqué y su nueva pareja.

Clara Chía tuvo que ser atendida de urgencia por un ataque de ansiedad en un centro hospitalario de Barcelona. Ni se quedó ingresada, ni está en terapia, solo fue atendida de urgencia. La novia de Piqué está superada y el acoso constante que sufre en las redes sociales le está pasando factura

Pero el hartazgo de Clara Chía, que tiene sus cuentas privadas, ha ido a más después de que sus padres y su hermana, a los que intenta proteger, también estén recibiendo ataques de los fans de Shakira. Y más allá de las redes, la hermana de Clara Chía, que es dos años menor que ella y vive en Barcelona, ha sido acosada recientemente por una televisión latinoamericana.

Comentario: Dado los hechos expuestos anteriormente se dice que existen varios factores a analizar el primero que el sujeto activo es muy diverso en esta figura delictiva e incluso incluyen varias personas como es el caso de que es una persona publica es acosada frecuentemente y por diferentes tipos de personas dando así la indefensión que tiene una persona dentro del ciberespacio, el segundo factor que se me hace interesante su análisis es la facilidad que tienen los acosadores en acceder a la información personal de la víctima, incluso dando acoso a su sector familiar como en este caso fueron a sus padres y hermana menor de edad. Frente a este acoso la víctima sufrió daño psicológico por lo cual tuvo que ser internada dando así un daño a la víctima producto de esta conducta.

Un tema bastante a estudiar es que el interés superior del niño es vulnerado en estos casos dado que si la persona en este caso es madre le causa daño también a estos, provocando a una indefensión de un grupo de atención prioritaria.

Caso #4

Link de la noticia: El acoso en redes a Joana Sanz, esposa de Dani Alves: "Hija de p***", "suicídate" o "eres cómplice de un violador" (lasexta.com)

Infractor: Sujeto activo: Grupo de personas las cuales son un número muy grande que acosan a Jhoanna Sanz, siendo una víctima colateral de un delito que ella no cometió, pero el esposo es un presunto sospechoso

Victima: Sujeto pasivo de género femenino, Joana Sanz esposa de Dani Alves que se lo acusa de presunta violación.

Hechos: Dani Alves ya ha cumplido una semana en prisión por agredir sexualmente a una joven en una discoteca de Barcelona. El futbolista aseguró en un primer momento que ni siquiera sabía quién era la joven, sin embargo, numerosas pruebas contra él han provocado que acabe reconociendo que mantuvo relaciones sexuales con ella, si bien afirma que fueron consentidas y que no llegó a decir la verdad por miedo a confesar la infidelidad a su mujer, Joana Sanz.

La presunta agresión tuvo lugar a principios de enero, sin embargo, el futbolista volvió a México, donde trabaja, tras lo sucedido. Las autoridades españolas estaban esperando a que volviera a España para detenerle, y fue cuando murió su suegra cuando pudieron hacerlo.

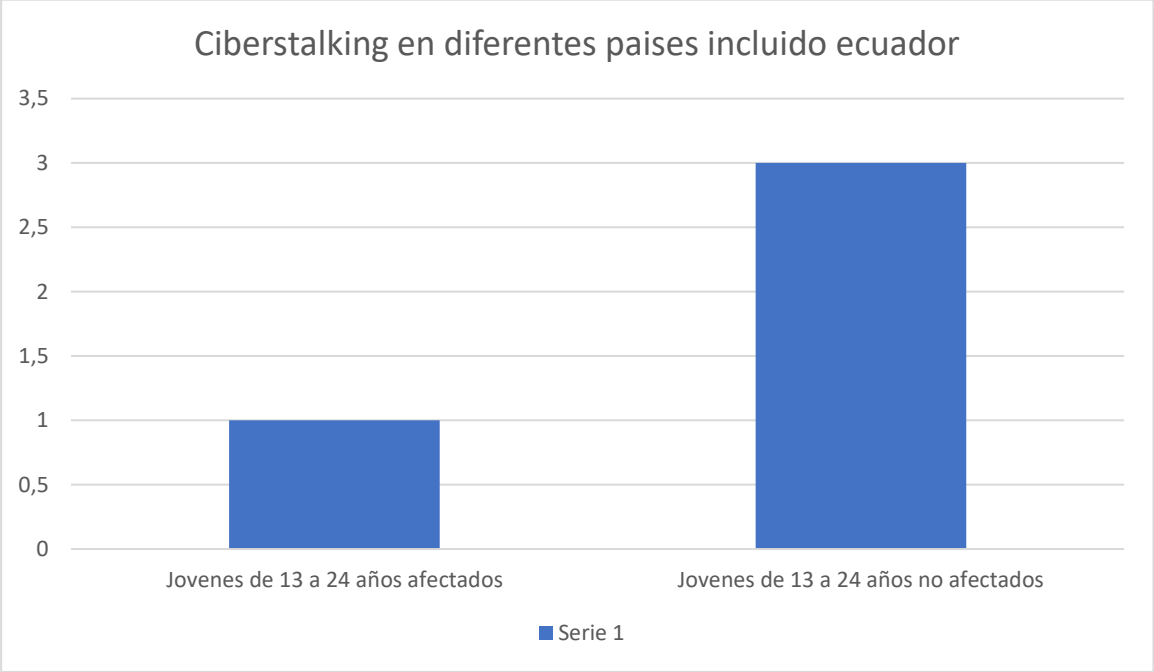
La esposa del futbolista está denunciando en sus redes sociales que, a pesar de ser una víctima colateral de lo sucedido, solo ha recibido amenazas en sus redes sociales, donde la tildan de "hija de p***", "pendeja" e incluso "cómplice de un violador".

Comentario: Dado los hechos expuestos anteriormente se dice que existen varios factores a analizar el primero que el sujeto activo es imposible de castigar dado los múltiples perfiles que escriben e incluso unos falsos dando así paso al anonimato del internet, el segundo punto a analizar es que si bien el sujeto pasivo no a hecho nada malo, a sido una víctima colateral producto de una acusación a su pareja, dando así una situación de miedo y molestia, como tercer punto de acuerdo al derecho comparado España cuenta con normativa que castiga estos actos los mismos ya sea por miedo o por desconocimiento dicha persona no denuncia.

6.4.Análisis datos estadísticos

Datos recolectados por la ONU el 4 de septiembre del año 2019

Gráfico #1



Fuente: Organización de las Naciones Unidas.

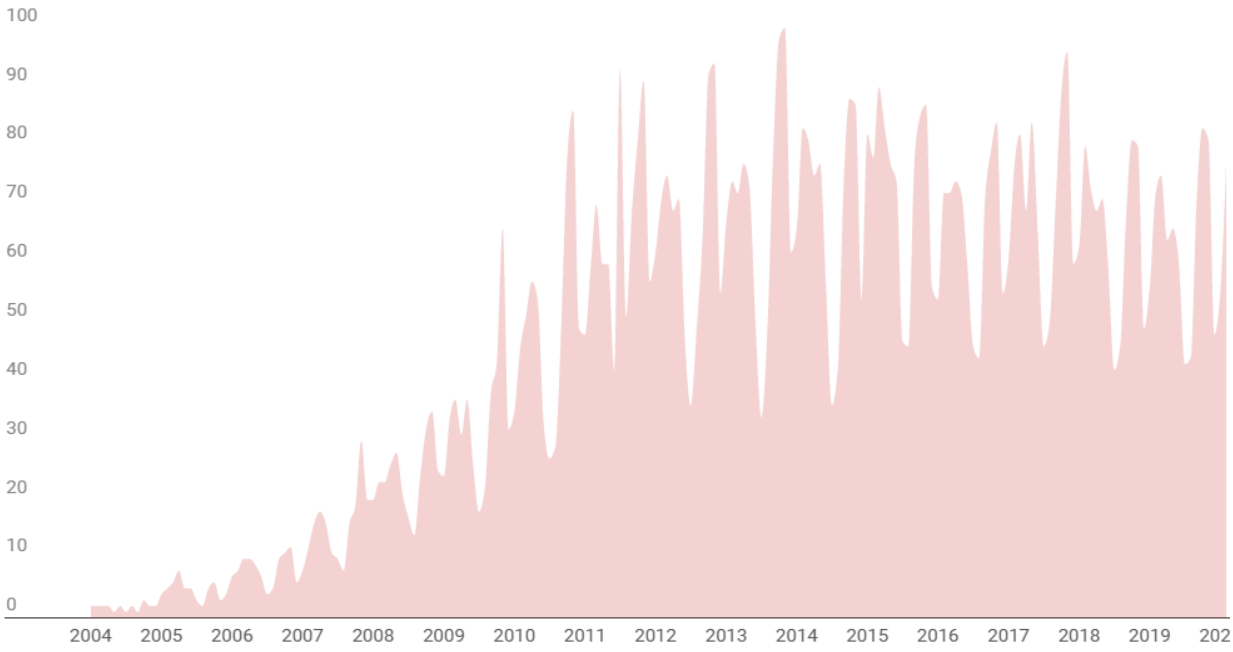
Autor: Miguel Ángel Benitez Guayllas.

Basado en afectados de 1 de cada 3 personas: Población encuestada de 30 países con un total de población encuestada de 170000

Comentario: En base a un estudio realizado por la Unicef y publicado en la pagina la la ONU, se dice que los encuestados en total son pertenecientes a más de 30 países y con un total de encuestados de alrededor de 170000 estudiantes pertenecientes a países como lo son Albania, Bangladesh, Belice, Bolivia, Brasil, Burkina Faso, Costa de Marfil, Ecuador, Francia, Gambia, Ghana, India, Indonesia, Iraq, Jamaica, Kosovo, Liberia, Malawi, Malasia, Malí, Moldavia, Montenegro, Myanmar, Nigeria, Rumania, Sierra Leona, Trinidad y Tobago, Ucrania, Vietnam y Zimbabwe. En el grafico se demuestra la existencia de este fenómeno en los años 2019 tiempos antes de pandemia Covid-19 los cuales si bien son 1 de cada 3 existe un problema social el cual debe ser solucionado. Este grafico demuestra una realidad que se vivió antes de

la necesidad de incluir aulas y virtualidad en su totalidad en los jóvenes y aun así existen gente que a sido víctima de esta nueva conducta

Gráfico #2



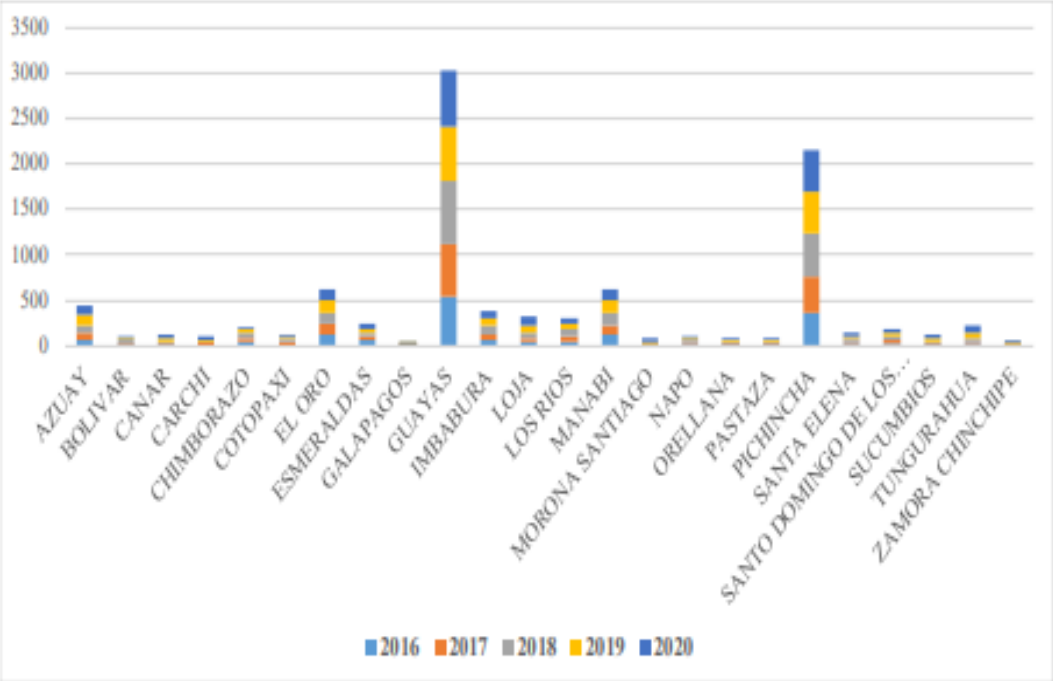
Fuente: Google trends

Autor: Miguel Ángel Benitez Guayllas

Comentario: Tal vez esta estadística sea algo rara pero la fuente que es Google trends es la base principal de Google en búsquedas la misma se trata de una herramienta gratuita proporcionada por Google que permite a los usuarios ver la popularidad relativa de un término de búsqueda a lo largo del tiempo y en diferentes ubicaciones geográficas.

La herramienta recopila datos de las búsquedas realizadas en el motor de búsqueda de Google y muestra los resultados en un gráfico de líneas que muestra el interés en un tema o término de búsqueda a lo largo del tiempo. Además, permite comparar el interés en varios términos de búsqueda y ver cómo ha cambiado su popularidad con el tiempo. Dando así la vista del inicie de interés o demostrando el impacto de esta nueva conducta en la sociedad, este grafico muestra datos recopilados desde el año 2004 hasta el año del 2020 que fue años donde fue inicios de la pandemia donde los índices de conductas delictivas usando redes sociales tuve su punto más alto hasta la actualidad dando asi la demostración que esta conducta ya es una realidad.

Gráfico #3



Fuente: Fiscalía general del Estado

Autor: Miguel Angel Benitez Guayllas.

Comentarios: En la presente estadística demuestra las denuncias y por ende también demuestra la realidad social de los ecuatorianos en el periodo de los años del 2016-2020 que han hecho denuncias frecuentes por el tema de acoso en línea, dando así que en lugares existan más o menos casos denunciados, tanto así que en la provincia del guayas es el mayor índice delincuencial de esta modalidad,

7. Discusión

7.1.Verificación de objetivos

Se procede a dar un análisis y aclarar los objetivos aprobados en el proyecto de investigación que fue presentado, los mismos que serán presentados a continuación.

7.1.1. Objetivo general

Realizar un estudio doctrinario respecto a la figura del ciberstalking

El objetivo general planteado en este proyecto de investigación se basa en el cometimiento de la figura del stalking, que es el acoso hacia una persona de forma reiterada el mismo que cumple unos requisitos específicos que lo hacen único como lo es la utilización de redes sociales al cual a esta nueva figura se la denomina ciberstalking, este objetico esta enfocado a analizar el cometimiento y su funcionamiento dentro del ciberespacio esta investigación se da gracias a diferentes criterios de autores nacionales como internaciones y así desarrollar los temas relacionados al mismo dentro del marco teórico se pudo obtener la evolución del delito de stalking en el país y a nivel internacional y a su vez la obtención de normativas del delito de stalking relacionándolo con otras figuras delictivas en el ámbito cibernético tratando de dar relación al mismo para adecuar su conducta al ciberstalking ya que son iguales a su actuación pero su medio y forma de actuar es lo que la hace única y algunas veces confundida, a su vez de realizar preguntas que ayuden a demostrar la existencia en la realidad social actual de la población ecuatoriana y demostrar que existe una impunidad de esta nueva figura delictiva.

7.1.2. Objetivos específicos

1.- Demostrar la existencia de la figura de ciberstalking en nuestra realidad y la impunidad de los delincuentes informáticos.

Este objetivo se da como realizado al momento de desarrollar las encuestas dando así una evidencia de esta nueva figura en la realidad ecuatoriana

2.- Realizar un estudio de derecho comparado en relación al delito de ciberstalking

Este objetivo se da como realizado al momento que lo abordamos en el marco teórico en el apartido de derecho comparado, pero como señale esta nueva figura delictiva parte desde un concepto ya establecido adecuándolo a las conductas nuevas como lo es la virtualidad.

3.-Proponer una propuesta de reforma al código orgánico integral penal respecto de la figura del ciberstalking.

Este objetivo se da como realizado en el apartado del proyecto de reforma legal en el mismo que se han señalado los considerandos y a su vez un artículo que señale la sanción y su conceptualización.

8. Conclusiones

Una vez terminado el análisis histórico, doctrinario al análisis de los resultados obtenidos en la investigación se puede obtener las siguientes conclusiones:

Primera. – La conducta del ciberstalking nace de una conducta física que es el stalking misma que la se la define como conducta dirigida repetitivamente contra un individuo concreto que este experimente como intrusiva o no deseada y que le cause miedo o intimidación, pero con el avance de las sociedad y la creación y avance de las nuevas tecnologías esta conducta al igual que otras se adaptó a las nuevas formas de conducta de los delincuentes, el mismo que actualmente a esta figura delictiva se la denomina con "ciberstalking" y al sujeto activo como "Stalker".

Segunda. - El cibersstalking, mismo que es realizado dentro de las redes sociales afectando a un sinnúmero de cibernautas, dando así paso a una nueva realidad dentro de la población ecuatoriana, la misma que al no ser un delito dentro del Código Orgánico Integral Penal se encuentra en un estado de impunidad el cual el sujeto activo "Stalker" se encuentra en un estado de superioridad frente al sujeto pasivo que es la víctima.

Tercero. – El anonimato es el principal problema dentro de los delitos cibernéticos, el mismo que no podrá ser resuelto en un periodo de tiempo largo, este problema y el internet que cada día se vuelve más global presenta un grave problema para la identificación del Stalker tanto así que en la actualidad existen muchos convenios, como lo es el convenio de Budapest, los mismos que dan conceptualización a diferentes figuras delictivas realizadas dentro del mundo virtual pero la persecución del sujeto activo es una odisea.

Cuarta. – La cooperación penal internacional es necesaria para la correcta persecución de los delincuentes que hagan uso de la virtualidad para realizar daño, engaños, amenazas, etc, pero como señale en el marco teórico de la presente investigación si bien las primeras dos fases para una correcta cooperación internacional son relativamente "sencillas" la parte que es la similitud normativa para aplicar una cooperación y armonía es un paso que actualmente los Estados enmarcados en su soberanía solo se la toma como una idea de una utopía.

Quinta. – Que, en la normativa actual, en el país no contamos con un enfoque en la identificación de las personas al momento de utilizar las redes sociales como medio para la actividad de realizar hechos delictivos como es la figura del ciberstalking

Sexto. -El avance tecnológico es un hecho y la utilización de las redes sociales como forma de comunicarse solo seguirá avanzando, esto nos hace llegar a la conclusión que sin una

correcta normativa y la adaptación del derecho al mundo virtual las nuevas formas de delitos, incluido el tema de esta investigación, seguirá avanzando.

Séptimo. – El delito denominado stalking llevado a la virtualidad usando redes sociales es un tema que es desconocido (Aunque la conducta y la modalidad que utilizan el Stalker no lo es) para la población ecuatoriana dada a la desinformación y su confusión con otros delitos dando así una sociedad indefensa antes estas actividades.

Octavo. – La idea de una identificación y verificación de usuario es una necesidad actual para dar un apoyo a la sociedad y por ende la identificación, y con ello llegar a una justicia, dado el uso que hacemos a las nuevas tecnologías de la información y comunicación (TIC) este requisito es un punto importante para el derecho penal informático y así una solución al anonimato,

Novena. – La jurisdicción surge como un nuevo problema al momento de tipificar esta nueva figura, dado que el mismo puede ser perseguido y juzgado en diferentes jurisdicciones dependiendo del país y su sistema legal dado que el uso de medios electrónicos trasciende fronteras, entonces para que pueda ser juzgado se basa en tres criterios los cuales son: Jurisdicción territorial, jurisdicción extraterritorial y jurisdicción basada en la ubicación del servidor.

Decima. – La competencia, como otro cualquier caso, es la facultad que tiene las autoridades competentes para conocer y resolver un caso en específico, en este sentido en los casos de delitos cibernéticos y enfocándonos en el cibertalking la competencia dependerá de la ubicación principalmente geográfica donde ocurrieron los hechos, y subsidiariamente la nacionalidad o residencia de la víctima y las leyes aplicables en uno otro caso, es estos casos deben existir dos tipos de competencias: competencia territorial y la competencia extraterritorial.

9. Recomendaciones

Luego del análisis de los resultados obtenidos en la investigación se recomienda lo siguiente:

- Que el Estado como ente protector y sancionador haga uso de las nuevas tecnologías de la información y comunicación con el fin de comunicar a la sociedad ecuatoriana de la normativa que actualmente está en uso en el Ecuador.
- Que el Estado haga uso de las redes sociales para informar el uso correcto de las mismas y los aparatos electrónicos con el fin de prevenir los acosos, amenazas y las nuevas actuaciones delictivas que se dan dentro de la misma.
- Que la Fiscalía general del estado informe a la ciudadanía sobre estos nuevos delitos de ciberstalking que se dan a través de las redes sociales con la finalidad de dar a conocer la forma de prevenir estas conductas.
- Que la asamblea Nacional mediante sus órganos legislativos busque y modifique la normativa legal vigente con respecto al delito del ciberstalking con el objetivo de garantizar los derechos establecidos en la Constitución como lo es el derecho al acceso a la información y el derecho a la reparación integral del daño.
- Se recomienda que se amplié el catálogo de delitos en el Código Orgánico Integral Penal y se incluya como figura individual al ciberstalking, pues es un hecho que el desarrollo de la delincuencia actual tiene un enfoque en el campo digital donde se le hace más fácil el vulnerar los derechos de la ciudadanía
- Que se le brinde importancia penal necesaria para el correcto uso de la defensa de los derechos vulnerados por la figura delictiva denominada “ciberstalking”.

9.1 Proyecto de reforma legal.

Propuesta de reforma jurídica al Código Orgánico Integral Penal (COIP)

Asamblea Nacional de la república del Ecuador

Considerando.

Que, El Ecuador es un Estado Constitucional de Derechos y Justicia y goza de supremacía constitucional.

Que, el numeral 2 del Artículo 16 de la Constitución nos dice que todas personas tienen derecho a el acceso universal a las tecnologías de la información y comunicación

Que, el Artículo 1 del Código Orgánico Integral Penal tiene la finalidad de normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas.

Que, se debe generalizar la utilización de servicios de redes de información e internet, de modo que éstos se convierten en un medio para el desarrollo de la educación comunicación y cultura.

Que, a través del servicio de redes electrónicas, incluidas la internet, se estableces relaciones sociales, informáticas y de comunicación las mismas que realizan actos que deben estar normados, regularlos y por ende controlarlos mediante una ley especializada en la materia.

Que, es indispensable que el Estado ecuatoriano cuente con herramientas jurídicas y acceder con mayor facilidad que le permitan el uso de los servicios electrónicos, incluido el uso de las redes sociales o cualquier otro medio de comunicación usando el internet, y acceder con mayor facilidad a las relaciones dentro de las redes sociales o las conexiones en el internet,

Por lo antes señalado y con el uso de la facultad que concede la Constitución de la República del Ecuador en su Art. 120 numeral 6 se plantea lo siguiente:

Código Orgánico Integral Penal

Que, a continuación del Art 154.3 agréguese el siguiente Art 154.4 que dirá:

Art 154.4 Ciberstalking. – La o las personas que acosen a otra persona a través de las tecnologías de la información y la comunicación, o por cualquier otro medio, con una finalidad que atente contra la dignidad de la persona, o con la finalidad de coartar su libertad o de generar un entorno intimidatorio, hostil, degradante, humillante u ofensivo, será castigado con la pena de prisión de tres meses a dos años.

Será castigado con la pena de prisión de seis meses a tres años si la conducta prevista en el apartado anterior se lleva a cabo contra una mujer por razón de su género.

Para la identificación del sujeto activo se usaran el registro de la tarjeta SIM si este se trata de celulares, o se usara la dirección IP si se trata de un dispositivo como computadora o dispositivos relacionados.

Disposición Final: La presente Ley Reformatoria al Código Orgánico Integral Penal entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado y firmado en la ciudad de San Francisco de Quito, Distrito Metropolitano, en la Sala de Sesiones de la Asamblea Nacional de la República de Ecuador, a los 22 días del mes de febrero del año 2023

f.…… f ……

Presidente de la Asamblea Nacional Secretario

10. Bibliografía

Albán, E. (2009). *Manual de derecho penal basico.*

BAUMANN, J. (1973). *Derecho penal conceptos fundamentales y sistema.* Buenos Aires: Depalma.

BETANCOURT, E. L. (2015). *Teoria del delito* . Ciudad de mexico: Porrua S.A.

Ecuador, C. d. (2008).

ESCAMILLA, A. A. (2018). *CIBERDELITOS.* Mar de Plata: hammurabi.

Garcia, E. H. (2015). *Apuntes de Introducción al derecho penal.*

González, J. A. (2013). *Delitos informaticos.* Nuevo Leon.

GREGORIE, M. (2001). *el cyberstalking es una extensión de la modalidad física.*

GUIONES, A. (2010). *La gestión de la identidad digital: una nueva habilidad.* Barcelona .

MACHICADO, J. (2010). *CONCEPTO DE DELITO.* Apuntes juridicos.

MARTIN, N. (2010). *El derecho penal europeo:una aproximación a sus problemas actuales.*

ORTEGA, J. (2016). *El ciberacoso y su relacion con el rendimiento academico.* Durango.

Panizo, S. R. (2009). *Los delitos informaticos* . Galicia.

Peña González, O., & Almanza Altamirano, F. (2010). *Teoría del Delito.* Lima - Perú: Asciación Peruana de ciencias Jurídicas y Conciliación.

Repubublica del Ecuador . (2022,16 de marzo). *Codigo Organico Integral Penal.* Registro oficial.

REYNOSO, T. (2014). *cyberbullyng, acoso cibernetico y delitos invisibles.* Toluca: Investigacion y estudios avanzados. .

RIQUERT, M. (2018). *CIBERDELITOS.* mar de plata: hammurabi.

ROMERO, M. (2021). *Derecho Penal del Enemigo Vs Derecho Penal del Ciudadano en el ordenamiento juridico ecuatoriano.* Macahala : Dominio de las ciencias .

SANCHEZ, P. (2015). *La teoria del delito* . Pamplona.

VALLEJO, V. (2010). *El delito informatico en la lgislacion ecuatoriana.* Quito: Corporación de estudios y publicaciones .

VILLANUEVA, R. (2004). *Teoria del delito.* Ciudad de Mexico: Instituto de investigaciones juridicas.

VILLVICENCIO, F. (2017). *DERECHO PENAL BASICO* . Lima: PUCP.

ZAFFARONI, E. (2000). *Derecho Penal Parte General.* Buenos aires: Sociedad Anonima Editora.

11. Anexos

Anexo 1. Oficio de designación del director de Trabajo Curricular

Universidad Nacional de Loja

SECRETARIA GENERAL
FACULTAD JURIDICA SOCIAL Y ADMINISTRATIVA

Presentada el día de hoy, tres de enero de dos mil veintitrés, a las doce horas con veintidós minutos. Lo certifica, la Secretaria Abogada de la Facultad Jurídica Social y Administrativa de la UNL.

ENA REGINA PELAEZ SORIA
Firmado digitalmente por ENA REGINA PELAEZ SORIA
Fecha: 2023.01.03 12:50:40 -05'00'

Dra. Ena Regina Peláez Soria, Mg. Sc
SECRETARIA ABOGADA DE LA FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

Loja, 03 de enero de 2023, a las 12H22. Atendiendo la petición que antecede, de conformidad a lo establecido en el **Art. 228 Dirección del trabajo de integración curricular o de titulación,** del Reglamento de Régimen Académico de la UNL vigente; una vez emitido el informe favorable de estructura, coherencia y pertinencia del proyecto, se designa al Dr. Freddy Ricardo Yamunaqué Vite, Ph. D., Docente de la Carrera de Derecho de la Facultad Jurídica Social y Administrativa, como **DIRECTOR del Trabajo de Integración Curricular o Titulación**, titulado: "INCLUIR LA FIGURA DEL CIBERSTALKING COMO DELITO EN EL CODIGO ORGANICO INTEGRAL PENAL Y SU PERSECUSION COMO FORMA DE ACOSO", de autoría del Sr. MIGUEL ANGEL BENÍTEZ GUAYLLAS. Se le recuerda que conforme lo establecido en el Art. 228 antes mencionado. Usted en su calidad de director del trabajo de integración curricular o de titulación *"será responsable de asesorar y monitorear con pertinencia y rigurosidad científico-técnica la ejecución del proyecto y de revisar oportunamente los informes de avance, los cuales serán devueltos al aspirante con las observaciones, sugerencias y recomendaciones necesarias para asegurar la calidad de la investigación. Cuando sea necesario, visitará y monitoreará el escenario donde se desarrolle el trabajo de integración curricular o de titulación".* **NOTIFÍQUESE para que surta efecto legal.**

MARIO ENRIQUE SANCHEZ ARMIJOS

Dr. Mario Enrique Sánchez Armijos, Mg. Sc.
DIRECTOR DE LA CARRERA DE DERECHO

Loja, 03 de enero de 2023, a las 12H23. Notifiqué con el decreto que antecede al Dr. Freddy Ricardo Yamunaqué Vite, Ph. D., para constancia suscriben:

FREDDY RICARDO YAMUNAQUE VITE

Dr. Freddy Ricardo Yamunaqué Vite, Ph. D.,
ASESOR DEL PROYECTO

ENA REGINA PELAEZ SORIA
Firmado digitalmente por ENA REGINA PELAEZ SORIA
Fecha: 2023.01.03 12:50:50 -05'00'

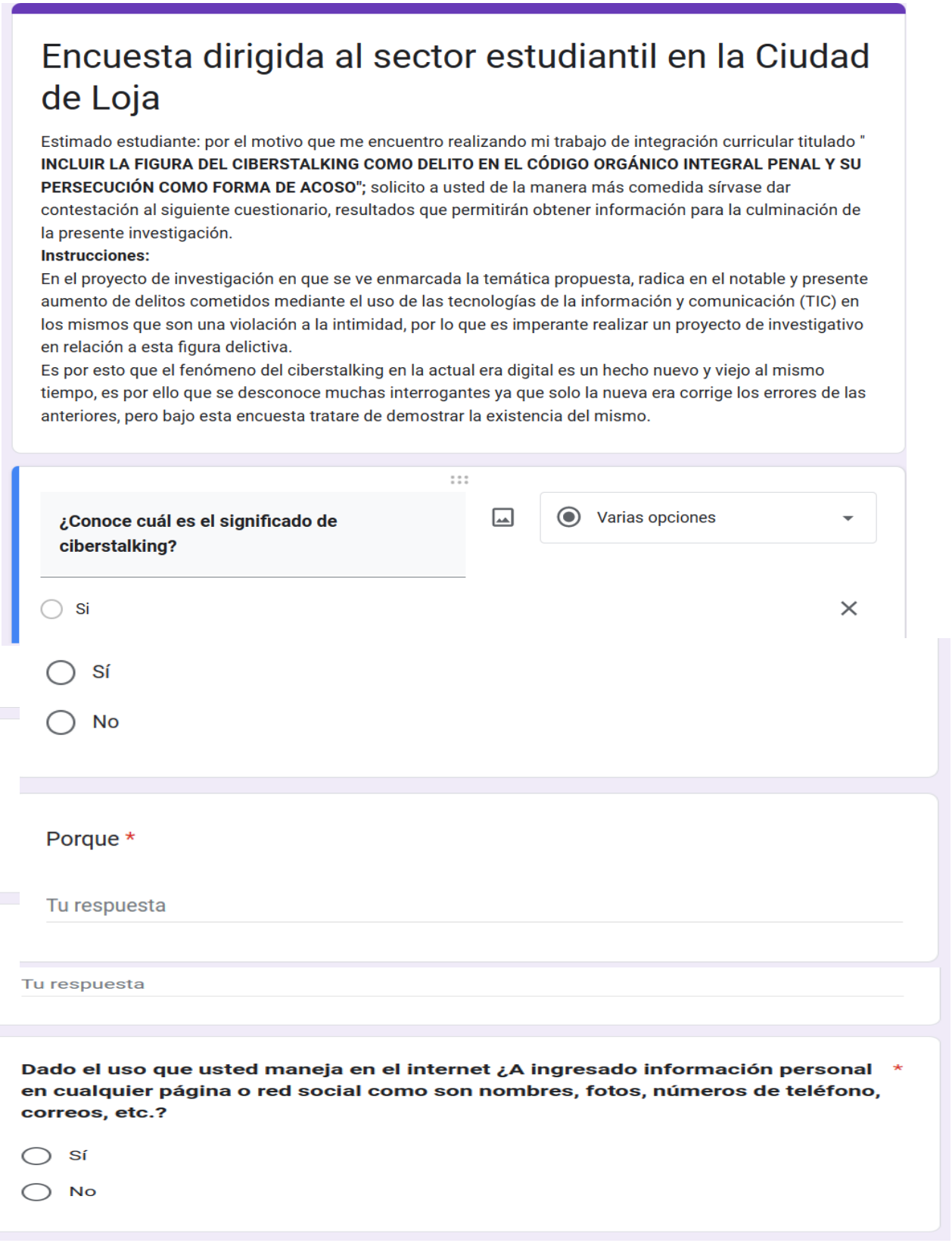
Dra. Ena Regina Peláez Soria, Mg. Sc.
SECRETARIA ABOGADA

NANCY MIREYA

Elaborado por: Nancy M. Jaramillo

C.C. *Sr. Miguel Ángel Benítez Guayllas*
Expediente de Estudiante

Anexo 2. Formato de Encuesta.



Encuesta dirigida al sector estudiantil en la Ciudad de Loja

Estimado estudiante: por el motivo que me encuentro realizando mi trabajo de integración curricular titulado " **INCLUIR LA FIGURA DEL CIBERSTALKING COMO DELITO EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL Y SU PERSECUCIÓN COMO FORMA DE ACOSO";** solicito a usted de la manera más comedida sírvase dar contestación al siguiente cuestionario, resultados que permitirán obtener información para la culminación de la presente investigación.

Instrucciones:

En el proyecto de investigación en que se ve enmarcada la temática propuesta, radica en el notable y presente aumento de delitos cometidos mediante el uso de las tecnologías de la información y comunicación (TIC) en los mismos que son una violación a la intimidad, por lo que es imperante realizar un proyecto de investigativo en relación a esta figura delictiva.

Es por esto que el fenómeno del ciberstalking en la actual era digital es un hecho nuevo y viejo al mismo tiempo, es por ello que se desconoce muchas interrogantes ya que solo la nueva era corrige los errores de las anteriores, pero bajo esta encuesta tratare de demostrar la existencia del mismo.

¿Conoce cuál es el significado de ciberstalking?

Varias opciones

Si

Sí

No

Porque *

Tu respuesta

Tu respuesta

Dado el uso que usted maneja en el internet ¿A ingresado información personal en cualquier página o red social como son nombres, fotos, números de teléfono, correos, etc.? *

Sí

No

Porque *

Tu respuesta

¿Ha tenido conocimiento o ha sido víctima de un acoso dentro de las redes sociales, como es mensajes de desconocidos, extraños o conocidos revisando constantemente su perfil e incluso recibir mensajes en cualquier medio de comunicación electrónico (Mensajes de WhatsApp, e-mails) de manera constante y por lo cual ha sufrido molestia o miedo? *

- ◯ Sí
- ◯ No

Porque *

Tu respuesta

¿Ha recibido algún tipo de amenaza, difamación, humillación, acoso sexual, invasión de la privacidad u otros comportamientos abusivos o agresivos? *

Anexo 3. Formato de la entrevista.

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA

CARRERA DE DERECHO

ENTREVISTA

Estimado profesional del Derecho: En razón de estar realizando mi Trabajo de Integración Curricular denominado: "**INCLUIR LA FIGURA DEL CIBERSTALKING COMO DELITO EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL Y SU PERSECUCIÓN COMO FORMA DE ACOSO**" le solicito de la manera más respetuosa se digne contestar las preguntas planteadas en esta entrevista. Sus respuestas me servirán para corroborar existencia y relevancia de figura del ciberstalking.

1.- El derecho de la comunicación e información, se encuentra en la C.R.E. en el artículo 16 en sus numerales 1 y 2 que estipula: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos. 2. El acceso universal a las tecnologías de información y comunicación., ¿Cree usted que el de acceso a estas redes debería ser controlado ya sea por el fiscal o la policía cibernética con la finalidad de prevenir la impunidad de los ciberdelincuentes?

2.- La falta de tipificación de esta figura en el derecho penal, ha llevado a una impunidad por no estar sujeta a una sanción que es el objetivo de la norma ¿Cree usted que es necesaria la tipificación de esta figura delictiva?

3.- El anonimato es uno de los principales problemas al momento de identificar al sujeto activo y por ende su sanción, ¿Se debería dar la potestad al fiscal para que pueda acceder a los dispositivos electrónicos de una persona si esta es sospechosa de cometer algún tipo de delito?

4 la figura denominada ciberstalking se la comete por medio del internet utilizando redes sociales o cualquier medio que se use para conectar a más cibernautas, por ende, este no es un problema nacional, ya que el Internet es a nivel mundial, según su criterio ¿Para controlar el comportamiento del ciberdelincuente, y por ende sea susceptible a una sanción o pena, se necesite la cooperación internacional?

5. El sujeto pasivo, la victima de esta figura delictiva del ciberstalking sufre daño moral, psicología e incluso daño físico, y por consecuencia la reparación integral son gastos que son pagados por la víctima, Según su criterio ¿El estado debería proporcionar el tratamiento gratuito a la víctima?

Anexo 4. Declaración de aptitud de titulación

Universidad Nacional de Loja

FACULTAD, JURIDICA SOCIAL Y ADMINISTRATIVA
SECRETARÍA GENERAL

DECLARATORIA DE APTITUD DE TITULACIÓN.

Ph.D.
Elvia Zhapa Amay.
DECANA DE LA FACULTAD JURÍDICA, SOCIAL Y ADMINISTRATIVA.

RESUELVO:

Conocido el informe emitido mediante Informe No. UNL-FJSA-SG-2023-0603 de 24 de marzo de 2023, por la Dra. Ena Regina Peláez Soria, Secretaria Abogada de la Facultad, en el que se establece que el **Sr. BENITEZ GUAYLLAS MIGUEL ANGEL** de nacionalidad ecuatoriana, con cédula Nro. **1150751855**, ha cumplido con los requisitos establecidos en el Art. 235 del Reglamento de Régimen Académico de la UNL en vigencia; me permito resolver:

Declaro la **APTITUD DE TITULACIÓN**, previo a la obtención del Título de **ABOGADO** en favor del **Sr. BENITEZ GUAYLLAS MIGUEL ANGEL.**

Notifíquese con el presente al interesado.

Loja, 24 de marzo de 2023.

Ph.D. Elvia Zhapa Amay.
DECANA DE LA FACULTAD JURÍDICA,
SOCIAL Y ADMINISTRATIVA.

C.C. ***Benítez Guayllas Miguel Ángel.***
Carrera de Derecho.
Secretaría General.
Expediente estudiantil.

Elaborado por: Abg. Karina Rojas J.

072 – 545174 ext. 21-23-28
Ciudad Universitaria **"Guillermo Falconí Espinosa"**
Casilla Letra "S" La Argelia. Loja – Ecuador

Página 2 | 2

Educamos para **Transformar**

Anexo 5. Certificado de traducción de Abstact.

BRENTWOOD LANGUAGE CENTER
Making a difference

Lic. Mónica Guarnizo Torres.
SECRETARIA DE "BRENTWOOD LANGUAGE CENTER"

CERTIFICA:

Que el documento aquí compuesto es fiel traducción del idioma español al idioma inglés del trabajo de titulación denominado **"Incluir la figura del ciberstalking como delito en el Código Orgánico Integral Penal y su persecución como forma de acoso"** del estudiante MIGUEL ÁNGEL BENÍTEZ GUAYLLAS, con cédula de identidad No. 1150751855, egresado de la carrera de Derecho de la Facultad Jurídica Social y Administrativa de la Universidad Nacional de Loja.

Lo certifica en honor a la verdad y autoriza a la interesada hacer uso del presente en lo que a sus intereses convenga.

Loja, 27 de julio de 2023

Lic. Mónica Guarnizo Torres
SECRETARIA DE B.L.C.

BRENTWOOD LANGUAGE CENTER
Making a difference

Dirección: Macará 12-27 entre Lourdes y Mercadillo (frente a las oficinas de Fedelibal)
Telf.: 2566002 - 0981896711 * Loja - Ecuador

Anexo 6. Certificado del tribunal de grado

Loja, 13 de Noviembre de 2023

EL TRIBUNAL DE GRADO CERTIFICA:

Que: Los integrantes del Tribunal de Sustentación y Calificación de Trabajo de Integración Curricular previo a dar cumplimiento con lo que dispone el Art. 236 del Reglamento de Régimen Académico de la Universidad Nacional de Loja, procedió a reunirse con la finalidad de socializar los contenidos del Trabajo de Integración Curricular presentado por el señor MIGUEL ÁNGEL BENÍTEZ GUAYLLAS, titulada "INCLUIR LA FIGURA DEL CIBERSTALKING COMO DELITO EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL Y SU PERSECUCIÓN COMO FORMA DE ACOSO", así como del articulo derivado de la misma.

Por tal motivo se autoriza la continuación de los trámites pertinentes para su publicación y sustentación pública.

PAZ PIEDAD RENGEL MALDONADO

Dra. Paz Piedad Rengel Maldonado Mg.Sc.
PRESIDENTE

JENNY MARITZA JARAMILLO SERRANO

Dra. Jenny Maritza Jaramillo Serrano, Mg. Sc.
MIEMBRO DE TRIBUNAL

ERIKA ANNABELL YAGUANA RODRIGUEZ
Firmado digitalmente por ERIKA ANNABELL YAGUANA RODRIGUEZ
Fecha: 2023.11.14 10:12:19 -05'00'

Abg. Érika A. Yaguana Rodríguez, Mg. Sc.,
MIEMBRO DE TRIBUNAL